المركز الديمقراطي العربي
برلين - ألمانيا

الجرائم الالكترونية
في الفقه الإسلامي والقانون الوضعي

جمع وتنسيق:
د. عباس حفصي

وقائع اعمال المؤتمر
الدولي الافتراضي
أيام 14 – 15 /ايار- مايو 2022

الجرائم الالكترونية في الفقه الإسلامي والقانون الوضعي

Democratic Arabic Center
Berlin - Germany











DEMOCRATIC ARABIC CENTER
Germany: Berlin 10315 Gensinger- Str: 112
http://democraticac.de
TEL: 0049-CODE
030-89005468/030-898999419/030-57348845
MOBILTELEFON: 0049174274278717






2022



المركز الديمقراطي العربي
للدراسات الاستراتيجية، الاقتصادية والسياسية
Democratic Arabic Center
for Strategic, Political & Economic Studies

كتاب وقائع المؤتمر العلمي الافتراضي:

الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in Islamic jurisprudence and positive law

إشراف وتنسيق:

د.عباس حفصي، جامعة الأغواط، الجزائر

د.حنان طرشان، جامعة باتنة1، الجزائر



النـــاشر:

المركز الديمقراطي العربي

للدراسات الإستراتيجية والسياسية والاقتصادية

ألمانيا/برلين

Democratic Arabic Center

Berlin / Germany

المركز الديمقراطي العربي

للدراسات الإستراتيجية والسياسية والاقتصادية ألمانيا/برلين

Tel: 0049-code Germany

030-54884375

030-91499898

030-86450098

البريد الإلكتروني

book@democraticac.de

المركز الديمقراطي العربي، برلين، ألمانيا

جامعة الجفرة، ليبيا

ينظمون المؤتمر الدولي الافتراضي السابع الموسوم بـ:

الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in Islamic jurisprudence and positive law

أيام 14-15 ماي 2022

إقامة المؤتمر بواسطة تقنية التّحاضر المرئي عبر تطبيق Zoom

ملاحظة: المشاركة مجانا بدون رسوم

الرئاسة الشرفية للمؤتمر:

أ. عمار شرعان، رئيس المركز العربي الديمقراطي، برلين، ألمانيا

د.يوسف أبوبكر جلالة، رئيس جامعة الجفرة، ليبيا

رئيس المؤتمر:

د.عباس حفصي، ليبيا

رئيس اللجنة العلمية للمؤتمر:

د. محمد عبد الحفيظ الشيخ، عميد كلية القانون، جامعة الجفرة، ليبيا

المنسق العام للمؤتمر:

د.أحمد بوهكو، رئيس تحرير المجلة الدولية للدراسات الإقتصادية

رئيس اللجنة التحضيرية للمؤتمر:

د.ناجية سليمان عبد الله، رئيسة تحرير مجلة العلوم السياسية والقانون

رئيس اللجنة التنظيمية للمؤتمر:

أ.كريم عايش، المركز الديمقراطي العربي، برلين، ألمانيا

مدير المؤتمر:

أ.كريم عايش، المركز الديمقراطي العربي، برلين، ألمانيا

التنسيق والنشر:

د.حنان طرشان، جامعة باتنة1، الجزائر

مدير إدارة النشر:

د.أحمد بوهكو، المركز الديمقراطي العربي، برلين، ألمانيا

أعضاء اللجنة العلمية:

د. زعادي محمد جلول، جامعة البويرة، الجزائر	د.برني كريمة، جامعة قسنطينة1، الجزائر
د.عالي حسن، جامعة سعيدة، الجزائر	د.نورس أحمد كاظم الموسوي، كلية المستقبل الجامعة
د.بوديبة رابح، جامعة سكيكدة، الجزائر	د.عدراء بن يسعد، جامعة قسنطينة!، الجزائر
د.دعاس آسيا، جامعة باتنة1، الجزائر	لوني تصيرة، جامعة البويرة، الجزائر
د.أحمد بوعون، كلية الحقوق، تونس	د.أمل فوزي أحمد عوض، جامعة حلوان، مصر
د.ميثم منفي كاظم العميدي، جامعة الكاظم، العراق	د.عبد القادر الشايط، جامعة محمد الأول، وجدة، المغرب
د.نبيل عبد الرحمن ناصر الدين إسماعيل، عضو هيئة التدريس، أكاديمية الشرطة، اليمن	د. هشام خلوق، جامعة عين الشق، المغرب

كلمة رئيس المؤتمر:

بسم الله الرحمن الرحيم:

معالي الدكتور/ يوسف أبوبكر جلالة رئيس جامعة الجفرة بليبيا الشقيقة

سعادة الدكتور عمار شرعان، رئيس المركز الديمقراطي العربي، برلين، بألمانيا

رئيس اللجنة العلمية، د.محمد عبدالحفيظ الشيخ عميد كلية الحقوق بجامعة الجفرة

رئيس اللجنة التحضيرية، الدكتورة ناجية سليمان عبد الله، رئيس تحرير مجلة العلوم الساسية والقانونية

المنسق العام، د. أحمد بوهمو

رئيس اللجنة التظيمية، أ. كريم عايش

أصحاب السعادة والسيدات والسادة رؤساء المشاركين في المؤتمر الدولي للجريمة الالكترونية

إن الجرائم بطبيعتها توجد بوجود الإنسان وتتطور بتطوره ، وما أن الإنسان دائما في تطور مستمر بفضل ثورة المعلومات والتكنولوجيا المتطورة فإننا نجد العلماء يحاولون الاستفادة منها، وبالمقابل نجد أن المجرمين يحاولون الاستفادة أيضا من التقدم التقني فأصبحت التكنولوجيا شيئا مباحا للحميع للصالح والطالح ، بل إن المجرمين كثر، واستطاعوا اكتساب خبرات ومهارات أكثر في تعاملهم مع الانترنت وارتكابهم للجرائم الإلكترونية عبر الأقمار الصناعية، ولم تعد جرائمهم تقتصر على إقليم دوله واحدة بعينها بل تجاوزت حدود الدولة، وهى جرائم متكررة ومستحدثة تمثل ضربا من ضروب الذكاء الإجرامي، استعصى إدراجها ضمن الأوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية، مما أوجب تطوير الأنظمة التشريعية الجنائية الوطنية بذكاء تشريعى مماثل للذكاء الإجرامى تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوائب تلك التقنيات وأبعادها الجديدة

ما يضمن في كافة الأحوال احترام مبدأ شرعية الجرائم والعقوبات من ناحية، ومبدأ الشرعية الإجرائية من ناحية أخرى، وتكامل في الدور والهدف مع المعاهدات والأنظمة الدولية، وهذا كله يمكن الوصول إلى سبل مواجهة هذه الجرائم الإلكترونية من حلال تعاون الأنظمة الدولية وفهمها للسبل الشرعية والعملل بها في مكاالفحة هذا النوع من الجرائم المتكررة والمستحدثة، فتكثر الاستفادة من هذه الوسائل والأجهزة الالكترونية، ويقل خطرها.

بدأت الثورة المعلوماتية نتيجة اقتران تقنيتي الاتصالات من جهة، والمعلومات وما وصلت إليه من جهة أخرى، فالثورة المعلوماتية هي الطفرة العلمية والتكنولوجية التي نشهدها اليوم، حتى بات يطلق على هذا العصر عصر المعلومات. وتعد المعلومة من أهم ممتلكات الإنسان التي اهتم بها على مر العصور، فجمعها ودونها وسجلها على وسائط متدرجة التطور، بدأت بجدران المعابد والمقابر، ثم انتهت باختراع الورق الذي تعددت أشكاله، حتى وصل بها المطاف إلى الحاسب الآلي والأقراص الإلكترونية المغنطة.

وقد تغني الأرقام عن الكثير من الأقوال، وأحيانا عن إيجاد مدخل مناسب عندما تزاحم العقل أفكارا عديدة ،ومنذ عقد مضى لم نكن نتصور إن الحياة سوف تعتمد بصفة أساسية ومطلقة على جهاز الحاسب الآلي وملحقاته، إلا أن ذلك أصبح واقعا وحقيقة، فمؤسسات الدولة تعتمد على الحاسب الآلي، والشركات العامة والخاصة كذلك، بل إن الأفراد في معاملاتهم الخاصة باتوا حريصين على التعامل معه و اعتماده في معاملاتهم بصورة تكاد تكون أساسية يمكن معها القول إن جهاز الحاسب الآلي أصبح يقاسم الإنسان حياته في نهاره وليله ونومه ويقظته، كيف لا وجهاز الحاسب الآلي في الطائرة وفي المعمل وفي القوات المسلحة وفي المواصلات والاتصالات على نحو يمكن معه القول إننا نعيش ثورة الحاسب الآلي. وقد تعززت منظومة الحاسب الآلي بالكمال بظهور شبكة المعلومات الدولية (الانترنت) والتي جعلت من العالم قرية صغيرة من حيث الأحداث والوقائع التي يمكن متابعتها في أي زمان ومكان، بل لحظة حصول الحدث ذاته.

ثم استتبع اتساع ونماء كل من تكنولوجيا الاتصالات والحاسبات من جهة، والبرمجية بما تضمنته من هندسة البرمجيات وصناعتها من جهة أخرى، والاندماج المذهل الذي حدث بينهما إلى الوصول إلى استحداث تقنية نظم المعالجة الآلية للمعطيات. لكن وعلى الرغم من المزايا الهائلة التي تحققت وتتحقق كل يوم بفضل الحاسب الآلي على جميع الأصعدة وفي شتى ميادين الحياة المعاصرة، فإن هذه الثورة التكنولوجية المتنامية صاحبتها في المقابل جملة من الانعكاسات السلبية والخطيرة جراء سوء استخدام هذه التقنية، ذلك أن الآثار الإيجابية المشرقة لعصر تقنية المعلومات لا تنف الانعكاسات السلبية التي أفرزتها هذه التقنية.

نتيجة إساءة استخدام الأنظمة المعلوماتية واستغلالها على نحو غير مشروع وبطرق من شأنها أن تلحق الضرر بمصالح الأفراد والجماعات، الشيء الذي استتبعه ظهور أنماط جديدة من الاعتداءات على تلك المعلومات المخزنة في بيئة افتراضية، ليس هذا فحسب بل سهلت هذه التقنية ارتكاب بعض الجرائم التقليدية، فازدادت هذه المخاطر تفاقما في ظل البيئة الافتراضية التي تمثلها شبكة المعلومات، مما أفرز نوعا جديدا من الجرائم، لم يكن معهودا من قبل عرفت بجرائم الحاسوب، أو الجرائم المعلوماتية.

والخطورة التي تتميز بها هذه الجرائم عن باقي الجرائم التقليدية تكمن في أنها سهلة الارتكاب نتيجة للاستخدام السلبي للتقنية المعلوماتية بما توفره من تسهيلات، وأن مرتكبي مثل هاته الجرائم لا ينتموا إلى زمرة المجرمين العاديين ذلك لأنهم يتسمون بالذكاء والدراية في التعامل مع مجال المعالجة الإلية للمعطيات والإلمام بالمهارات والمعارف التقنية، فضلا على أن آثارها ليست محصورة في النطاق الإقليمي لدولة بعينها بل تشمل جميع دول العالم على اعتبارها متصلة ببعضها البعض بواسطة الشبكة العالمية للمعلومات.

وكما تكمن الخطورة كذلك من عدة نواحي، وعلى سبيل الذكر لا الحصر نذكر من الناحية الأخلاقية أن مثل هاته الجرائم تستهدف فضح الأسرار الشخصيّة أو القذف أو التشهير بشركات أو أشخاص بقصد الإضرار بالسمعة الشخصية أو المالية .ولعل أبرز الجرائم المتواجدة حاليا على مستوى الأنظمة المعلوماتية ومن خلال الانترنت نجد تجارة الدعارة و والصور الخليعة والاستغلال الجنسي بكل صوره التي أصبحت أكبر التجارات المتواجدة حاليا على الشبكة العنكبوتية، وأصبحت تؤرق جل دول المعمورة من أجل محاربتها .ولقد أجريت دراسات حول علاقة مثل هاته الجرائم

عن باقي الجرائم الأخرى ،حيث وجد أن الجرائم تزداد اطرادا مع الجرائم الأخرى، وكثير من الدول سواء المتقدمة او غير المتطورة باتت تشتكوا من مثل هذه المواقع التي تبث هاته الافكار.

ومع الخطورة الأخلاقية نجد كذلك هناك خطورة مجتمعية حيث قد لا يدُرك كثيرون أنّ الجماعات المتطرّفة كانت من أولى الجماعات الفكريّة التي استخدمت الحاسوب ودخلت العالم الإلكتروني حتى قبل أنْ تظهر شبكة الإنترنت بسنوات، مما أصبح يهدد مجتمعات بأسرها. ومع الغموض الذي يكتنف جرائم الحاسوب حيث أصبحت تثير بعض التحديات القانونية والعملية أمام الأجهزة المعنية بمكافحة الجريمة (أجهزة العدالة الجنائية بجميع مستوياتها وعلى اختلاف أدوارها)، وبالذات فيما يخص إثبات هذه الجرائم وآلية مباشرة إجراءات الاستدلال والتحقيق عبر البيئة الافتراضية لتعقب المجرمين وتقديمهم للعدالة.

إن هذا الغموض الذي يصاحب هاته الجرائم جعل مجال البحث فيها يضيق بل جعل الكثير من الفقهاء سواء من الناحية الشرعية أو القانونية يترددون في إعطاء حكم شرعي أو تجريم بصورة واضحة، ومع ذلك حاول المشرع القانوني وكذا فقهاء الشريعة الإسلامية مسايرة هذا التطور لهذا النوع من الجرائم.

أيها السادة والسيدات: المشاركون الكرام

إننا وبكل فخر واعتزاز، نرحب بكم مجددا وآمل أن نستفيد من هذا المؤتمر على كافة الأصعدة والمستويات

في الأخير، وإذ أتشرف برئاسة هذا المؤتمر أجدد شكري وعرفاني لكل من ساهم في إنجاح هذا المؤتمر من قريب أو بعيد...

شكرا على حسن الإصغاء

والسلام عليكم ورحمة الله،

رئيس المؤتمر:

د.عباس حفصي، جامعة الأغواط، الجزائر



ديباجة المؤتمر:

إن الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت. ويمكن وبحسب البيئات والوسائل المختلفة المستخدمة، تحدث الجريمة الإلكترونية دون تواجد الجاني في مكان الحدث، وتستند الطريقة المستخدمة إلى تكنولوجيا الاتصالات والمعلومات الحديثة. إن عدد الجرائم الالكترونية في انتشار واسع نظرا للتطور الحاصل في التكنولوجيا سواء في وسائل التواصل الاجتماعي آو عبر الدول مما أضر باقتصادها ومختلف تعاملاتها، كما أن الأساليب الإجرامية اختلفت وتنوعت من قبل متمرسين في هذا الجانب.

وبما أن الشريعة رادعة في جانب العقوبات فاشتملت على عقوبات توقف كل مجرم يتجاوز حدود الله تعالى ويسعى في الأرض فسادا والله لا يحب المفسدين. وجاء القانون أيضا معاقبا كل من تسول له نفسه الاعتداء على حقوق الناس بالسلب أو النهب أو الظلم.

كما أن هناك عدة انواع للجرائم الالكترونية وتتمثل في سرقة الهوية حيث يقوم فيها المجرم بإغراء الضحية واستخراج المعلومات منه بشكل غير مباش، واستهداف المعلومات الخاصة من أجل الربح واستغلالها لتحقيق مكاسب مادية وأيضا تهديد الأفراد حيث يقوم المجرم، من خلال القرصنة وسرقة المعلومات، بالوصول إلى المعلومات الشخصية الخاصة بالضحية، ثم ابتزازهم لكسب المال وتحريضهم على ارتكاب أعمال غير قانونية قد يتعرضون فيها للظلم.

وكذلك من الأنواع التشهير حيث يستخدم المجرم المعلومات المسروقة ويضيف اليها معلومات كاذبة ثم يرسلها عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني لكثير من الناس بهدف تشويه سمعة الضحية وتدميرها نفسياً.وغيرها من الأنواع المتعددة في هذا المجال.

إن خطر الجريمة الالكترونية خطر عظيم تجاوز كل الحدود والأعراف وأصبح يهدد الأشخاص والدول، لذا وجب الحد من هذا التفاقم المتزايد بمعاقبة المجرمين عقابا صارما دون تردد أو تأخير. الجريمة الالكترونية يصعب اثباتها جراء التعقيدات التي في ثناياها لان من السهولة اخفاء دليل اثباتها لذلك يجد المحققون صعوبة جمة في اثبات أدلة الجريمة.

إشكالية المؤتمر الدولي:

- ✓ ما هو موقف الشريعة الاسلامية والقانون الوضعي من الجريمة المعلوماتية؟
- ✓ ماهي الطرق المنوطة بإثبات هاته الجرائم؟
- ✓ كيفية تعامل الجهات المختصة مع هذا النوع من الجرائم؟
- ✓ ماهي الحلول الممكنة للحد من هاته الجرائم وسبل مكافحتها؟
- ✓ ما مدى مواكبة المشرع العربي للقوانين المعاصرة في مجال المعلوماتية

أهداف المؤتمر الدولي:

- ✓ الجريمة الالكترونية ماهيتها ومعرفة أسبابها وأركانها
- ✓ الجريمة الالكترونية وسبل مكافحتها
- ✓ موقف الشريعة الإسلامية من الجريمة المعلوماتية.
- ✓ إثبات الجريمة من الناحية الشرعية والقانونية.
- ✓ مواكبة النصوص العقابية في القانون للنصوص في الشريعة الاسلامية.
- ✓ التعرف على تجارب الدول الأخرى في ردع أصحاب هاته الجرائم.
- ✓ مدى مواكبة نصوص القوانين العقابية في الدول العربية للدول المتقدمة في هذا الجانب.

محاور المؤتمر:

المحور الأول: الإطار العام للجريمة الالكترونية

- ✓ تعريف الجريمة الالكترونية وأركانها.
- ✓ أسباب ارتكابها
- ✓ طبيعتها وخصائصها

المحور الثاني: مواجهة الجرائم الالكترونية وطرق إثباتها

- ✓ الإثبات الشرعي والقانوني للجريمة الالكترونية
- ✓ طرق مواجهة الجرائم الالكترونية
- ✓ شروط وطرق الإثبات الالكتروني

المحور الثالث: الجرائم المتصلة بالجرائم الالكترونية

- ✓ جريمة القذف والتشهير الالكتروني
- ✓ جريمة السرقة الالكترونية
- ✓ جريمة النصب والاحتيال الالكتروني
- ✓ جريمة التزوير الالكتروني
- ✓ الإرهاب الالكتروني

المحور الرابع: دور مختلف المؤسسات في مكافحة الجريمة الالكترونية

- ✓ المحاكم والقضاء
- ✓ النيابة العامة
- ✓ المخابر الجنائية

فهرس المحتويات

جريمة تزوير التوقيع الالكتروني

Electronic signature fraud

د.عباس حفصي/ جامعة الأغواط /الجزائر
Dr.abbas hafsi/ University of Laghouat/Alger

ملخص الدراسة:

تتنوع الجرائم المرتكبة من خلال استخدام الإنترنت، بما في ذلك الجرائم التي تنطوي على المال، وكذا الجرائم البشرية، والجرائم ضد الممتلكات، وحقوق التأليف والنشر والاختراع. إن جرائم الاستخدام عبر الإنترنت تهدد الأمن الداخلي للبلاد من خلال الوصول الى اهم قواعد البيانات، وكذلك الجرائم ضد الأمن الخارجي للبلاد، وكذلك الجرائم التي تمس المعاهدات أو الجرائم ذات الطابع الدولي، مثل الجرائم الإرهابية.

الكلمات المفتاحية: الجرائم، التزوير، الانترنت، الأمن الداخلي، الخارجي، الطابع الدولي، العقوبة، الظرف المشدد، عقوبة الشروع، الاتفاق الجنائي

Abstract:

Crimes committed through the use of the Internet are diverse, including crimes involving money, human crimes, crimes against property, copyright and invention. , The crimes of using the Internet threaten the internal security of the country through access to the most important databases, as well as crimes against the external security of the country, as well as crimes that affect treaties or crimes of an international nature, such as terrorist crimes.

Keywords: Forgery, the Internet, internal and external security, the international character, the penalty, the aggravating circumstance, the penalty of attempt, the criminal agreement

أولا-تعريف التوقيع الالكتروني:

عرفه المشرع الفرنسي في المادة 4/1316 على انه التوقيع الذي يحدد شخصية من هو منسوب إليه والذي يفصح عن قبوله بمضمون المحرر الذي يرتبط به وبالالتزامات الواردة فيه. (نصيرات، 2005، ص. 24)

وتجدر الإشارة إلى أن المشرع الفرنسي أصدر توجيهًا خاصًا حدد فيه التوقيعات العادية بوظائفها، ثم التوقيعات الإلكترونية، وكأنه أراد تحديد وظائف التوقيعات الإلكترونية على أساس التوقيعات العادية، إلا أنه لم يفعل ذلك. تحديد الطريقة التي يتم بها اعتماد التوقيعات الإلكترونية، ولكنه يشترط أن تكون هذه طريقة لتحديد هوية الموقع بشكل موثوق والتأكد من ارتباط التوقيع بالعمل أو المستندات المتعلقة به.

1.تعريف المشرع الجزائر:

للوقوف على ضوابط وأحكام التوقيع الالكتروني والتصديق أصدر المشرع الجزائري القانون رقم 04/15 المؤرخ في 1 فيفري 2015 الذي يحدد القواعد العامة المتعلقة بالتوقيع والتصديق الالكترونيين، فإنهم يتفقون على أن

التوقيعات الإلكترونية هي استمرار لمجموعة من الوسائل الإجرائية أو التقنية، سواء كانت رمزية أو رقمية أو مشفرة، مصممة لإخراج رسالة لصاحبها علامة فريدة. يأتي هذا التوقيع الإلكتروني، الذي يُنقل إلكترونيًا، بأشكال عديدة اعتمادًا على طريقة معينة من الواضح أنه مع كل التعاريف السابقة للتوقيعات الإلكترونية، فإن المبرمجين الجزائريين لم يتناولوا تعريف التوقيعات الإلكترونية، وهناك تقارب في التعريفات الأخرى في التعريفات التي قدمتها كل دولة. كذلك، باستثناء أنه لا يوجد شامل تعريف للتوقيع الإلكترون، وقد يكون ذلك بسبب التطور السريع لوسائل الاتصال والذي بدوره يؤدي إلى تغير التعريف في كل مرة. (بيومي، 2002، ص.72)

2.خصائص التوقيع الالكتروني عن التوقيع العادي:

يختلفان من عدة نواحي منها:

تحدد معظم التشريعات شكل التوقيع المكتوب كما يظهر عادة في التوقيع أو الختم أو بصمات الأصابع. أما بالنسبة للتوقيع الإلكتروني، فإن التشريع الصادر لا يحدد الصورة المحددة للتوقيع الإلكتروني، ولكنه يسمح له بأن يتخذ أي شكل، سواء كان ذلك في شكل صور أو أحرف أو أرقام أو رموز أو إشارات أو حتى أصوات، طالما لها خصائص فريدة يمكن تمييزها: الشخص الذي يوقع على التوقيع، ويتعرف عليه ويعرب عن رغبته في الموافقة على عمل قانوني أو الاكتفاء بمضمونه. (عبد الحميد، 2002، ص.52)

الوسيط المستخدم في التوقيع المكتوب هو عادة دعم ورقي مرفق بالتوقيع الكتابي. أما بالنسبة للتوقيعات الإلكترونية، فالوسطاء هم وسائط الكترونية من خلال أجهزة الكمبيوتر والإنترنت (عبد الحميد، 2002، ص.52-51)

يمكن لأي شخص تسجيل الدخول كتابيًا بعدة طرق، مثل التوقيع أو الختم أو بصمة الإصبع، ويمكن استبدال أي من هذه الطرق بالطرق الأخرى، على عكس التوقيع الإلكتروني، الذي يتم فقط بطريقة واحدة محددة مسبقًا وبناءً على المسموح به بإجراءات تقنية الأمان لاستكمال تحديد هوية الموقع، وضمان عدم العبث بأمان المحرر أو تشويهه. (الأباصيري، 2002، ص. 79).

3.أنواع التوقيع الإلكتروني:

أ-التوقيع الرقمي:

هذا النوع من التوقيع الإلكتروني هو محتوى رقمي مطبوع تشكل المعلومات الإلكترونية في النهاية توقيعًا الكترونيًا، والذي يتميز أيضًا باستخدام مفتاح للتشفير يمكنه تحويل الأرقام والرموز التي تشكل التوقيع إلى معادلات ورموز غامضة للقراءة فقط من قبل الأشخاص المرتبطين بالعلاقات القانونية، 1 يتم استخدام هذه الصورة خاصة في المعاملات المصرفية والشركات (جمال، 2017، ص.11).

ب. التوقيع بالقلم الالكتروني:

استخدم الموقّع في هذه الصورة قلم ضوئي خاص لكتابة توقيعه عليها شاشة كمبيوتر بها برنامج يلتقط التوقيعات ويتحقق منها بناءً على الحركة، ثم يتم نقل القلم والشكل الذي يرسمه إلى الماسح الضوئي (الماسح الضوئي) ينقل الصورة إلى المحرر للتوقيع الإلكتروني، وهذه الصورة متمايزة، لكن من الأسهل التزييف على أساس أن الأشخاص

ذوي الخبرة هم مجرمون يمكنهم كسر التوقيع بسهولة، لذلك تعتقد النظرية القانونية أن هذه الصورة لا تحقق الأمان الكافي (جمال، 2017، ص.20-21)

ج . التوقيع البيومتري:

يعتمد هذا النوع على الإحساس الذاتي بالموقع، مثل بصمات الأصابع، والقزحية، والنغمة الصوت ... تتم العملية بأخذ بصمة الإصبع أو قزحية العين وتخزينها على جهاز الكمبيوتر هي آلية ومشفرة، أي تحمها من الآخرين بالرغم من التكلفة العالية لهذه التقنية ومع ذلك، فإنه لا يوفر الحماية المطلوبة للتوقيعات الإلكترونية، حيث تتغير هذه المعاني من عملية إلى عملية الحوادث التي قد تُفقد فيها، على سبيل المثال، بصمات الأصابع تمامًا بسبب حريق قد يتعرض له الموقع. (الملوم، 2011، ص.125-126)

د. التوقيع باستخدام البطاقة الممغنطة المقترنة بالرقم السري:

تستند هذه الصورة إلى جهاز كمبيوتر متصل بالأنترنت مملوك للموقع الشيء الجميل في الأمر أنه لا يتطلب خبرة للحصول على هذا النوع من التوقيع. وتجدر الإشارة إلى أن هذا التوقيع شائع جدًا، خاصة في المعاملات المصرفية، ليتم إرفاقه يمتلك العملاء كلمة مرور تحتوي على أرقام وحروف ورموز تمكنهم من سحب الأموال وإيداعها للدفع مقابل السلع والخدمات، يُدخل الموقع كلمة المرور الخاصة به في فتحة الجهاز جهاز الصراف الآلي، إذا كانت كلمة المرور صحيحة ستظهر البيانات على شاشة الجهاز يحدد موقع الويب كمية السلع أو الخدمات (محمد، 2013، ص.71).

4. حجية التوقيع الالكتروني:

أ.بالنسبة للقانون الفرنسي:

أصدر المشرع الفرنسي اللائحة رقم 271 98 التي تنظم المعاملات القانونية والسلوك في مجال التأمين الصحي، والتي يتم فيها الاعتراف بالتوقيعات الإلكترونية التي يتم إجراؤها من خلال استخدام بطاقات التأمين الصحي الإلكترونية، وتكون المؤسسات الوطنية ملزمة بالاعتراف بالتوقيعات الإلكترونية. (رمضان، 2001، ص.29)

لكنه أصدر القانون رقم 230 الصادر في 13 مارس من عام 2000 م الخاص بالتجارة الإلكترونية والمعاملات الإلكترونية.

كما نص في أحكام القانون على أن التوقيع الإلكتروني يحدد هوية الموقع ويضمن علاقته بالأحداث المنسوبة إليه ويؤكد هويته وصحة الأحداث التي ينسب إليها التوقيع حتى يثبت العكس. (سعيد، 2005، ص.25)

لذلك، أعطى المشرع الفرنسي الحجية بشكل كامل للكتابة الإلكترونية والوثائق الإلكترونية والتوقيعات الإلكترونية، تمامًا مثل المستندات الورقية والكلمات المكتوبة والتوقيعات المكتوبة بخط اليد.

ب. القانون الجزائري:

ذكر المشرع الجزائري في المادة 327 (2) من القانون المدني الجزائري (2/327) على أن التوقيعات الإلكترونية يجب أن تؤخذ في الاعتبار بموجب الشروط المنصوص عليها في المادة 323 مكرر (1) من نفس القانون. حتى الآن، حيث ساوى المشرع بين صحة التوقيعات التقليدية والتوقيعات الإلكترونية، وهو ما يسمى التكافؤ الوظيفي بين التوقيعين، لأن التوقيعات الإلكترونية يمكن أن تؤدي نفس وظيفة التوقيعات التقليدية لتحديد هوية الموقّع. حيث أنه يجب ان

تكون موقعة عليها ويمكن تمييزها عن غيرها على النحو المبين في القانون النموذجي لعام 1996 بشأن التجارة الإلكترونية في التعامل مع التوقيعات الإلكترونية، الذي يذكر فكرة إيجاد الوسائل التقنية لتحقيق نفس المفهوم والغرض مثل التوقيعات العادية.

ثانيا-أركان جريمة تزوير التوقيع الالكتروني:

جريمة تزوير التوقيع الالكتروني تتكون من الركن المادي والمعنوي:

الركن المادي:

تعد جريمة تزوير التوقيع الإلكتروني من الجرائم التي تخص محتوى التجارة الإلكترونية نفسها وليس بياناتها، لأن عقد التجارة الإلكترونية سواء كان عقد بيع أو عقد استيراد أو عقود أخرى يتطلب صلاحيته. مثل عقد التجارة التقليدي، لدى كلا الطرفين توقيعات كاملة عليه، وتوقيع عقد التجارة الإلكترونية هو توقيع إلكتروني، وجريمة التزوير في ركنه الأساسي هي تغيير أصالة المستند بالطريقة التي يحددها قانون. طريقة لإيذاء الآخرين.

يتمثل عنصر جريمة تزوير التوقيع الإلكتروني في تغيير حقيقة ما يلي: من شأنه أن يضر بالمصالح الشخصية، لذلك تتطلب هذه الركيزة مجموعة العنصر هي:

أ.تغيير الحقيقة:

تغيير الوقائع أساس جريمة التزوير، فبدون هذا الركن لا تقع جريمة التزوير، فإذا أثبت أحدهما أن البيانات مطابقة للوقائع، فلا تقع جريمة التزوير حتى لو كان الشخص. يعتقد أن هذه البيانات غير صحيحة، حتى لو أفعاله ويمكن أن يحدث هذا أيضًا عندما يقوض حقوق الآخرين.

عند تغيير الحقائق، سواء كانت وثائق رسمية أو عرفية، يمكن تخيل صحة هذه الوثائق ضمن حدود المعلوماتية، والتي تُعرف في هذه الحالة باسم جريمة تزوير المعلومات، والتي تعتبر بمثابة تغيير في المستندات والوثائق الإعلامية التي تتم معالجتها تلقائيًا هم. (قهوجي، 1992، ص.62)

يتم تعريف ملف المعلومات على أنه كل كيان منفصل أو يمكن فصله عن نظام معالجة المعلومات الآلي والذي يتم تسجيل معلومات معينة عليه، سواء كان الغرض منه الاستخدام بواسطة نظام معالجة مؤتمت أو مشتق من هذا النوع.

ب. طرق التزوير:

ب 1. جريمة صنع أو حيازة برنامج لإعداد توقيع الكتروني مزور:

وهو ماجاء في المادة 394 مكرر قانون العقوبات: "يعاقب بالحبس من ثلاثة أشهر إلى سنة وبغرامة من 50000 إلى 100000 دج كل من يدخل أو يبقى عن طرق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك" تضاعف العقوبة إذا ترتب عن ذلك حذف أو تغيير لمعطيات المنظومة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة "تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 إلى 150000 دج".

كما جاء في المادة 02 من الاتفاقية الدولية للإجرام المعلوماتي.

الصورة البسيطة للجريمة تتمثل في مجرد الدخول أو البقاء غير المشروع فيما الصورة المشددة، تتحقق بتوافر الظرف المشدد لها، ويكون في الحالة التي ينتج فيها عن الدخول أو البقاء غير المشروع إما محو أو تغيير في المعطيات الموجودة في النظام أو تخريب لنظام اشتغال المنظومة.

1. الصورة البسيطة:

أ-فعل الدخول:

الدخول هنا لا يعني الدخول بالمعنى المادي، أي الدخول إلى مكان أو منزل أو حديقة، في نفس اتجاه الكمبيوتر، ولكن يجب أن يُنظر إليه على أنه ظاهرة أخلاقية، على غرار ما نعرفه. مثل إدخال فكرة أو قدرة تفكير الشخص. أي وصول إلى العمليات العقلية التي تقوم بها أنظمة معالجة البيانات الآلية. لم يحدد المشرع وسيلة الدخول أو طريقة الدخول إلى النظام، لذا فإن أي طريقة أو طريقة حدثت فيها الجريمة من شأنها أن ترقى إلى الدخول المباشر أو الدخول غير المباشر. (قهوجي، 1992، ص.121)

ب-فعل البقاء:

قد يتخذ النشاط الإجرامي الذي يشكل العنصر المادي للجريمة قيد الدراسة في ظل تواجده في النظام، في حين أن الغرض من فعل البقاء هو الدخول إلى نظام معالجة البيانات الآلي ضد إرادة الشخص المرخص له. يمكن التحكم في هذا النظام ومعاقبته للبقاء داخل النظام بشكل مستقل عن نظام الدخول، وقد يلتقيان، البقاء قديكون مستقلاً عندما يكون الدخول إلى النظام قانونيًا، على سبيل المثال: إذا كان الدخول إلى النظام عرضيًا أو خاطئًا أو إهمالًا، في هذه الحالة يجب عليه قطع تواجده والخروج فورًا، كما لايُعاقب بالإقامة غير القانونية إذا كان ذلك له عنصر أخلاقي.

ويكون البقاء جريمة إذا تجاوز المتدخل المدة المسموح بها للبقاء بداخل النظام، أو في الحالة التي يطبع فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيه الرؤية والإطلاع فقط ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات التلفونية، والتي يستطيع فيها الجاني الحصول على الخدمة التلفونية دون أن يدفع المقابل الواجب دفعه أو يحصل على الخدمة مدة أطول من المدة التي دفع مقابلها عن طريق استخدام وسائل أو عمليات غير مشروعة، وقد يجتمع الدخول غير المشروع والبقاء غير المشروع معا وذلك في الفرض الذي لا يكون فيه الجاني الحق في الدخول إلى النظام، ويدخل إليه فعلا ضد إرادة من له حق السيطرة عليه، ثم يبقى داخل النظام بعد ذلك، ويتحقق في هذا الفرض الاجتماع المادي للجرائم و إذا كانت تلك الجريمة على هذه الصورة تهدف أساسا إلى حماية نظام المعالجة الآلية للمعطيات بصورة مباشرة، إلا أنها تحقق أيضا و بصورة غير مباشرة حماية المعطيات أو المعلومات ذاتها بل يمكن من خلالها تجريم سرقة وقت الآلة ، وذلك بالنسبة للموظف أو العامل أو غيرهما حين يسرق وقت الآلة ضد إرادة من له الحق السيطرة على النظام، و يقوم بطبع أو نسخ بعض المعلومات أو المعطيات أو البرامج (قارة، 2006، ص.111).

كما يمكن تطبيقه على الاستخدام غير القانوني للبطاقة المغنطة، سواء تم استخدامها بعد سرقة أو تزوير البطاقة المغنطة، أو حتى إذا استخدم المالك البطاقة المغنطة لسحب المبلغ عندما يكون الرصيد غير كاف، أو عندما

لا يكون هناك التوازن، فإنه يشكل جريمة في هذه الحالة. هي جريمة الحجز غير القانوني في النظام بشرط أن يعلم حامل البطاقة مقدمًا أنه لا يملك رصيدًا كافيًا، ويمكن أيضًا تطبيقه على المكالمات الهاتفية التنصت على المكالمات الهاتفية، طالما يتم معالجة رقم الهاتف تلقائيًا في النظام الخاص. تعتبر هذه الجريمة جريمة فعل مجردة، أي أنها تشكل فعلاً يقع ويكتمل بمجرد وقوعه، أي يدخل أو يبقى في غياب مشرع، في شكله القانوني، يتطلب أي نتيجة جنائية وفقاً مع أحكام الإدانة الجنائية (قارة، 2006، ص.114).

2 . الصورة المشددة:

جاء في المادة 394 مكرر 3/2: " تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظمة وإذا ترتب عن الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة أشهر إلى سنتين والغرامة من 50000 دج إلى 150000 دج".

جاء في المادة 394 مكرر 3/2 من قانون العقوبات على حالتين تكون فيهما عقوبات جريمة الدخول إلى النظام والبقاء فيه شديدة، عندما يؤدي الإدخال أو الإقامة إلى حذف أو تعديل البيانات الواردة في النظام. النظام أو النظام غير قادر على أداء وظيفته ويكفي لإثبات وجود علاقة سببية بين الدخول غير القانوني أو الإقامة غير القانونية والنتيجة الضارة، والتي لا تتطلب أن تكون النتيجة الضارة متعمدة لأنه سيكون من غير المعقول طلب مثل هذا شرط لأن المشرعين جعلوها جريمة قائمة بذاتها محاولة مهاجمة نظام عن طريق محو أو تعديل البيانات التي يحتوي عليها. كما أن هذه النتيجة لا تتطلب الإهمال المتعمد أي الإهمال غير المتعمد، فالظرف المشدد هنا هو ظرف مادي كافٍ لوجوده بينه وبين الجريمة الأساسية المتعمدة، أي جريمة. يُقال إن الدخول أو الإقامة، علاقة سببية، موجود، ما لم يثبت الجاني أن العلاقة غير موجودة. على سبيل المثال، إذا ثبت أن تعديل البيانات أو حذفها، أو عدم قدرة النظام على أداء وظائفه ناتج عن قوة قاهرة أو حادث.

أ . الاعتداء العمدي على سير نظام المعالجة الآلية للمعطيات:

تنص المادتان 05 و08 من الاتفاقية الدولية لجرائم المعلومات على أن المشرع الجزائري لم يقدم نصًا لهجمات متعمدة على وظائف النظام. الهجمات على البيانات والأنظمة بناءً على ما إذا كان الهجوم وسيلة أو غرضًا يشكل جريمة مهاجمة البيانات عمداً. (فشار، 2006، ص.27)

الهجمات على عمليات النظام بسبب الدخول أو الإقامة غير القانونية ليست بالضرورة مقصودة، ولكن المشكلة هي أن الهجمات على عمليات النظام بسبب الدخول القانوني يمكن أن تمر دون عقاب، خاصة إذا لم يكن هناك دخول قانوني. أحكام للهجمات المتعمدة على وظائف النظام.

يتجلى هذا السلوك الجسدي على أنه سلوك يمنع نظام معالجة البيانات التلقائي من أداء أنشطته العادية والمقصودة، أو السلوك الذي يعطل نشاط أو وظيفة ذلك النظام. إنه يؤثر فقط على عنصر واحد من هذه العناصر، سواء كان الكمبيوتر المادي نفسه، أو شبكات الاتصال، أو معدات الإرسال ... إلخ، كما هو الحال بالنسبة للأصول غير الملموسة مثل البرامج والبيانات.

ب .الاعتداءات العمدية على المعطيات:

تتطرق إليها المواد08،04،03 من الاتفاقية الدولية للإجرام المعلوماتي، كما ذكرها المشرع الجزائري في المادة 394 مكرر2 في قانون العقوبات:"يعاقب بالحبس من ستة أشهر إلى ثلاث سنوات و بغرامة من 500000 دج إلى 2000000 دج كل من أدخل بطريقة الغش معطيات في نظام المعالجة الآلية أو أزال أو عدّل بطريقة الغش المعطيات التي تتضمنها".

الصورة الأولى: الاعتداءات العمدية على المعطيات الموجودة داخل النظام ويتمثل النشاط الجرمي في الصور التالية:

الإدخال-المحو-التعديل:

لا يشترط ان تجتمع هاته الصور مرة واحدة، ويكفي للمخالف أن ينشر إحداها لتلبية متطلبات العنصر المادي. الإدراج والحذف والتعديل الذي يتضمن التلاعب بالبيانات الموجودة في أنظمة معالجة البيانات الآلية، سواء عن طريق إضافة بيانات جديدة أو غير صحيحة أو حذف أو تعديل بيانات موجودة مسبقًا، يعني أن النشاط الإجرامي في هذه الجريمة هو الموقع أو الموضوع هو بيانات أو معلومات تتم معالجتها تلقائيًا لتصبح رمزًا أو رمزًا يمثل تلك المعلومات، بدلاً من المعلومات نفسها كأحد عناصر المعرفة، ويقتصر موقع هذا النشاط الإجرامي على البيانات داخل النظام، أي تلك التي تحتوي على بيانات وتشكل جزءًا من النظام. (فشار، 2006، ص.28)

لا تقتصر الجريمة على المعلومات التي لم يتم إدخالها في النظام أو التي تم إدخالها ولم تتم معالجتها تلقائيًا، كما هو الحال بالنسبة لما يتم معالجته، حتى لو لم تتم معالجته بعدما أصبح يتمتع بالحماية الجنائية، والتي يمكن أن يقال إنها جنائية صريحة أو محاولة، حسب الظروف.

وتجدر الإشارة إلى أن الحماية الجنائية تشمل البيانات ما دامت واردة في نظام المعالجةالآلي، أي ما دامت واردة في ذلك النظام وهي وحدة ومكوناتها، ولا تتحقق الجريمة في حالة حدوث النشاط الإجرامي على البيانات خارج النظام ، سواء كانت داخل النظام أو شخص يدخل النظام قبل أو بعد خروجه، أو دخول شخص ما بعد الخروج منه، ولا يحتاج لإجراء عمليات مباشرة لإدخال البيانات ومسحها وتعديلها، ولكن يمكنه القيام بذلك بشكل غير مباشر ، سواء عن بعد أو من خلال شخص ثالث وعمومًا التلاعب في المعطيات الموجودة داخل النظام يتخذ إحدى الأشكال التالية (فشار، 2006، ص.29) :

- الإدخال:

يهدف السلوك الوارد إلى إضافة بيانات جديدة إلى دعمها، إما فارغة أو مع البيانات السابقة، حيث يتم إدخال أرقامه الخاصة والسرية لسحب مبلغ يتجاوز المبلغ الموجود من حسابه، وكذلك صاحب حق البطاقة الائتمانية التي دفع من خلالها أكثر من المبلغ المحدد له، سواء من صاحبها الشرعي أو غيره في حالة السرقة أو الضياع أو التزوير، وعملية الدخول في كل حالة تقدم برنامجًا غريبًا يضيف بيانات جديدة "فيروسات ... إلخ".

- المحو:

عملية المسح تعني حذف أو إتلاف جزء من البيانات المسجلة على الدعامة داخل النظام، أو نقل وتخزين جزء من البيانات إلى منطقة الذاكرة.

- التعديل:

تعديل السلوك يعني تغيير البيانات داخل النظام واستبدالها ببيانات أخرى ، ومحو السلوك وتعديله يتم تحقيقه من خلال برامج غريبة عن طريق التلاعب بالبيانات، سواء بشكل كامل أو جزئي، أو باستخدام برامج البيانات والمحاة أو القنابل المعلوماتية لبرامج الفيروسات، وقد تم ذكر أعمال الإدراج والحذف والتعديل هذه على وجه التحديد ، ولا ينبغي تجريم أي أعمال أخرى، حتى لو تضمنت هجومًا على البيانات داخل نظام معالجة البيانات تلقائيًا ، وبالتالي فإن فعل نسخ البيانات ، وعملية نقل البيانات ، وفعل تنسيق ، أو جمعهم معًا ، لأن كل هذه الأفعال لا تتضمن إدخالًا أو تعديلًا بالمعنى السابق.

- الصورة الثانية: المساس العمدي بالمعطيات خارج النظام: (حفصي، 2015، ص.153)

وفر المشرع الجزائري الحماية الجزائية للمعطيات في حد ذاتها من خلال تجريمه السلوكات التالية:

1- نص المادة 394 مكرر2 يستهدف حماية المعطيات في حد ذاتها لأنه لم يشترط أن تكون داخل نظام المعالجة الآلية للمعطيات أو أن يكون قد تم معالجتها آليا، فمحل الجريمة هو المعطيات سواء كانت مخزنة كأن تكون مخزنة على أشرطة أو أقراص أو تلك المعالجة آليا أو تلك المرسلة عن طريق منظومة معلوماتية، ما دامت قد تستعمل كوسيلة لارتكاب الجرائم المنصوص عليها في القسم السابع مكرر من قانون العقوبات.

2- نص المادة 394 مكرر 2/2 يجرم أفعال الحيازة، الإفشاء، النشر، الاستعمال، أيا كان الغرض من هذه الأفعال التي ترد على المعطيات المتحصل عليها من إحدى الجرائم الواردة في القسم السابع مكرر من قانون العقوبات بأهداف المنافسة غير المشروعة، الجوسسة، الإرهاب، التحريض على الفسق ...الخ.

3. الركن المعنوي:

جريمة التزوير نوع من الجرائم العمدية التي تتطلب وجود النية الإجرامية كأساس للركن االمادي حيث يجب أن تكون إرادة الجاني موجهة لارتكاب الفعل الذي يشكل جريمة في جريمة التزوير لا بد ان تكون هناك نية خاصة لا بد من وجودها، أي ضرورة قيام الجاني بالتحقق في النية. والغرض المحدد هو استخدام المستند لغرض التزوير، بحيث يكون الركن المادي لجريمة التزوي، التزوير هو تكون عنصرين، إرادة التصرف ونية استخدام الوثائق المزورة، والتزوير قد يكون مادياً وقد يكون معنوياً، ولكل نوع طرقه الخاصة، فالتزوير المادي هو الذي يقع بوسيلة مادية يتخلف عنها أثر يدرك حسياً سواء في مادة المحرر أو في شكله.

أما التزوير المعنوي فهو الذي يقع بتغيير الحقيقة دون أن يترك ذلك أثراً يدرك بالحس، والتزوير المادي قد يقع وقت إنشاء المحرر أو بعد ذلك، بينما التزوير المعنوي لا يقع إلا وقت إنشاء المحرر. (حفصي، 2015، ص.155)

4.الضرر:

يعتبر الارتباط بالوجود وعدم الوجود في الضرر كركن هام من عناصر جريمة التزوير ونقصد بذلك إلى الضرر المباشر، أي فقدان المنفعة المحمية قانونًا.

5 . العقوبة في تزوير التوقيع الالكتروني:

وفقًا للمواد 11 و12 و13 من القانون الجنائي والاتفاقية الدولية لجرائم المعلومات، يجب أن تكون العقوبات المنصوص عليها في جرائم المعلومات رادعة، بما في ذلك عقوبات الحرمان من الحرية، والعقوبات الأصلية والتكميلية المطبقة على الأشخاص الطبيعيين. والأشخاص الاعتباريين. (عاقلي، 2017)

1. العقوبات المطبقة على الشخص الطبيعي:

أ. العقوبات الأصلية:

عقوبة الحبس تتراوح مدتها من شهرين إلى ثلاثة سنوات، حسب الفعل المرتكب والغرامة تتراوح قيمتها من خمسين ألف دج إلى خمسة مائة ألف دج، حسب الفعل المرتكب: الدخول والبقاء بالغش (الجريمة البسيطة)، الدخول والبقاء بالغش (الجريمة المشددة) وتضاعف العقوبة إذا ترتب عن هذه الأفعال حذف أو تغيير لمعطيات المنظومة، الاعتداء ألعمدي على المعطيات.

ب.العقوبات التكميلية:

المصادرة تشمل الأجهزة والبرامج والوسائل المستخدمة في إرتكاب الجريمة من الجرائم الماسة بالأنظمة المعلوماتية، مع مراعاة حقوق الغير حسن النية. وإغلاق المواقع والأمر يتعلق بالمواقع (les sites) التي تكون محلا لجريمة من الجرائم الماسة بالأنظمة المعلوماتية، وإغلاق المحل أو مكان الاستغلال إذا كانت الجريمة قد ارتكبت بعلم مالكها ومثال ذلك إغلاق المقهى الالكتروني الذي ترتكب منه مثل هذه الجرائم شرط توافر عناصر العلم لدى مالكها.

ت-عقوبة الشروع في الجريمة:

جاءت به المادة 11 من الاتفاقية الدولية للإجرام ألمعلوماتي واعتمده المشرع الجزائري بالنسبة للجرائم الماسة بالأنظمة المعلوماتية، بحيث توسع نطاق العقوبة لتشمل أكبر قدر من الأفعال الماسة بالأنظمة المعلوماتية، إذ أصبح الشروع معاقب عليه بنفس عقوبة المقررة على الجنحة ذاتها.

ث -الظروف المشددة:

نص القانون على ظرف تشدد به عقوبة جريمة الدخول والبقاء غير المشروع داخل النظام، ويتحقق هذا الظرف عندما ينتج عن الدخول والبقاء إما حذف أو تغيير المعطيات التي يحتويها النظام وإما تخريب نظام اشتغال المنظومة، تضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات العامة.

2-العقوبات المطبقة على الشخص المعنوي:

يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا أو شريكا أو متدخلا كما يسأل عن الجريمة التامة أو الشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه أو ممثليه.

وبالتالي عقوبة الشخص المعنوي تتمثل في الغرامة التي تعادل خمس مرات الحد الأقصى المقرر للشخص الطبيعي 40علما أن نص المادة 18 مكرر من القانون 15/04 المتضمن قانون العقوبات تحدد المسؤولية الجزائية للشخص المعنوي والعقوبات المقررة.

3-عقوبة الاتفاق الجنائي:

تبنى المشرع الجزائري مبدأ معاقبة الاتفاق الجنائي بنص المادة 394 مكرر 5، بغرض التحضير للجرائم الماسة بالأنظمة المعلوماتية، وعقوبة الاشتراك في الاتفاق تكون نفس عقوبة الجريمة التي تم التحضير لها فإذا تعددت الجرائم تكون العقوبة هي عقوبة الجريمة الأشد.

النتائج:

- ✓ هناك عدة تعريفات للتوقيع الالكتروني غير ان المشرع الجزائري لم يعط تعريفا له
- ✓ هناك عدة خصائص للتوقيع الالكتروني وأنواع تم التطرق اليها في البحث
- ✓ يعتبر المشرع الجزائري التوقيعات الإلكترونية يجب أن تؤخذ في الاعتبار بموجب الشروط المنصوص عليها في المادة 323 مكرر (1).
- ✓ ساوى المشرع بين صحة التوقيعات التقليدية والتوقيعات الإلكترونية.
- ✓ تقوم جريمة التزوير الالكتروني على الركن المادي الذي يقوم على تغيير الحقيقة بطرق التزوير المعروفة بالصورة البسطية والمشددة.
- ✓ تقوم جريمة التزوير الالكتروني على الركن المعنوي الذي يتطلب وجود النية الإجرامية.
- ✓ تقوم جريمة التزوير الالكتروني على الضرر المباشر الذي من خلاله تفقد المنفعة.
- ✓ العقوبات في جريمة التزوير الالكتروني هي عقوبة الحبس تتراوح مدتها من شهرين إلى ثلاثة سنوات كعقوبة أصلية.
- ✓ والعقوبة التكميلية المتمثلة في المصادرة وتشمل الأجهزة والبرامج والوسائل المستخدمة في إرتكاب الجريمة.
- ✓ عقوبة الشروع أصبح معاقب عليه بنفس عقوبة المقررة على الجنحة ذاتها.
- ✓ عقوبة الشروع تضاعف العقوبة إذا استهدفت الجريمة الدفاع الوطني أو الهيئات والمؤسسات العامة
- ✓ عقوبة الاتفاق الجنائي بنص المادة 394 مكرر 5 وهي نفس عقوبة الجريمة التي تم التحضير لها.

قائمة المراجع:

1) قارة، أمال. (2006). الحماية الجزائية للمعلوماتية في التشريع الجزائري.د.م: دار هومة.
2) عبد الحميد، ثروت. (2002). التوقيع الالكتروني. القاهرة: دار الجامعة الجديدة
3) حجازي، بيومي. (2002). التجارة الالكترونية ونظامها القانوني.
4) ديلمي، جمال. (2017). الإطار القانوني للتوقيع والتصديق الإلكترونيين في الجزائر. كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو.
5) رمضان، مدحت عبد الحليم. (2001). الحماية الجنائية للتجارة الالكترونية. القاهرة: دار النهضة العربية
6) حفصي، عباس. (2015). جرائم التزوير الالكترونية. أطروحة دكتوراه، جامعة وهران، الجزائر
7) نصيرات، علاءمحمد. (2005). حجية التوقيع الالكتروني دراسة مقارنة. القاهرة: دار الثقافة للنشر
8) الغريب، فيصل سعيد. (2005). التوقيع الالكتروني وحجيته في الاثبات. د.م.: د.ن.

9) الأباصيري، فاروق محمد أحمد. (2002). عقد الاشتراك في قواعد المعلومات. القاهرة: الدار الجامعية الجديدة للنشر

10) فشار، عطالله. (2006). المعالجة الالية للمستندات.الجزائر: الدرا الجامعية

11) عاقلي، فضيلة. (2017). الجريمة الإلكترونية وإجراءات مواجهتها من خلال التشريع الجزائري. تم الاسترداد من مركز جيل البحث العلمي: http://jilrc.com/%D8%A7%D9%84%D8%AC%D8%B1%D9%8A%D9%85%D8%A9-%D8%A7%D9%84%D8%A5%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-%D9%88%D8%A5%D8%AC%D8%B1%D8%A7%D8%A1%D8%A7%D8%AA-%D9%85%D9%88%D8%A7%D8%AC%D9%87%D8%AA/#:~:text=%D8%A7%D9%84%D9%85%D9%84%D8%AE%D8

12) قهوجي. (1992). الحماية الجنائية لبرامج الحاسب. الإسكندرية: الدار الجامعية للطباعة والنشر

13) لملوم، كريم. (2011). الإثبات في معاملات التجارة الإلكترونية بين التشريعات الوطنية والدولية. كلية الحقوق والعلوم السياسية، رسالة ماجستير، الجزائر

14) نص المادة 2/327. (بلا تاريخ).

15) محمد، نصر محمد. (2013). الدليل الإلكتروني وحجيته أمام القضاء. بيروت: دار الكتب العلمية.

الجريمة الإلكترونية عبر مواقع التواصل الاجتماعي في القانون المغرب

Electronic crime via social networking sites in Moroccan law

ط.د. محمد المبطول/جامعة محمد الخامس، الرباط / المغرب

PhD. Mohamed Al-Matbol/Mohammed V University, Rabat/Morocco

ملخص الدراسة:

لقد شهد العالم تطورات كبيرة في جميع المجالات والميادين خاصة الميدان التكنولوجي، فمن الأبواب التي طرقتها هذه التطورات نجد تكنولوجيا وسائل الإعلام والاتصال، فبالرغم من حداثة العهد بهذه التكنولوجيا في مجتمعنا، إلا أنها ودون منازع استطاعت أن تفرض وجودها في حياة كل فرد، فقد ساهم التطور المعاصر في تبادل الأفكار والمعلومات إلى إحداث سلوكيات مقبولة وغير مقبولة، في جميع المجالات التي تتعلق بالفرد والمجتمع، وقد أدى الاستخدام المفرط لهذه المواقع والمنصات إلى بروز أنماط جديدة من الجريمة، في ظل قصور وسائل الرقابة وضعف التشريعات القانونية فرض العقوبة لتحجيم تأثيرات هذا النوع من الجرائم. مما دفع المشرع المغربي كغيره في التجارب المقارنة إلى محاولة ضبط هذه المواقع عبر وضع قوانين تأطرها، ولاسيما بواسطة التجريم والعقاب.

الكلمات المفتاحية: الجريمة الإلكترونية، مواقع التواصل الاجتماعي، القانون، المغرب

Abstract:

The world has seen significant developments in all fields and fields of special technological field. It is the doors where these developments will find media and communication technology. Contemporary in exchange of ideas and information to make acceptable and unacceptable behaviors, in all areas relating to individual and society. The excessive use of these sites and platforms has led to the emergence of new types of crime, under the palaces of control and weak legal legislation to enforce the impact of this type of crime. Which prompted the Moroccan legislator as other in comparative experiments to try to adjust these sites by putting fraudulent laws, especially by criminalization and punishment.

KeyWords : Cybercrime, social media, law, Morocco

مقدمة:

أدى التطور الذي عرفته البشرية على مستوى وسائل الاتصال وتقنية المعلومات والشبكة العنكبوتية "الإنترنت" إلى تقريب المسافات، وجعل العالم قرية صغيرة رغم شساعته وامتداده، وذلك من خلال إتاحته لإمكانية التواصل عن بعد بين ملايين من الأشخاص على مدار الساعة وبشكل مباشر دون اعتبار للحدود الجغرافية، وتعتبر فضاءات الحوار الاجتماعي أكثر المواقع الالكترونية التفاعلية استعمالا في السنوات السابقة.

ولقد سمحت تكنولوجيا المعلومات والاتصال عموما ومواقع التواصل الاجتماعي وما في حكمها على وجه الخصوص بمساحات شاسعة من حرية الرأي والتعبير لأوسع الشرائح الاجتماعية، وتوارت العديد من الأبعاد وتلاشت مجموعة من القيود أمام هذه الحرية ولم تصمد أمام قوة وجبروت التقنية والتكنولوجيا.

وأمام هذه المساحات الشاسعة للتعبير والتعليق والانتقاد والموالاة وغيرها من المواقف طرح سؤال المسؤولية عند ممارسة هذه الحقوق والحريات.

فبالرغم من الإيجابيات والتسهيلات التي جاءت بها مواقع التواصل الاجتماعي، إلا أن لها العديد من السلبيات التي ألحقت أضرارا بالمجتمع، من خلال إساءة استعمالها فتحولت هذه الفضاءات من أماكن للتعارف والتواصل وتنمية المهارات الفكرية والإبداعية إلى أماكن خصبة لارتكاب الجرائم وملاحقة الأفراد والإساءة لهم، فلم يقف الأمر على مضايقة الأشخاص والتعرض لهم وإنما وصل إلى درجة تهديد أمن الدولة وسلامة ترابها.

وهكذا أصبح الاستخدام الآمن لهذه المواقع حتمية ضرورية وهاجسا أمام رجال القانون والمشرعين، خاصة مع الوتيرة المتسارعة لتداول المعلومات والاستخدام العشوائي لمواقع التواصل وقصور وسائل الرقابة وضعف التشريعات القانونية وفرض العقوبة لتحجيم تأثيرات هذا النوع من الجرائم التي تستهدف الأفراد والدول.

وتهدف هذه المداخلة التي تندرج ضمن المحور الثالث "الجرائم المتصلة بالجرائم الإلكترونية" إلى الكشف عن موقع الجريمة عبر مواقع التواصل الاجتماعي في التشريع المغربي، وكذا الوقوف على مكامن القوة والضعف في هذا القانون لمواجهة هذه الجرائم، إضافة إلى التعرف على الآليات التشريعية والمؤسساتية لمكافحة هذا النوع الجديد من الجريمة، وذلك عبر الخوض في الإشكالية الرئيسية التالية: **"إلى أي حد استطاع المشرع المغربي وضع سياسة جنائية واضحة وملائمة لمكافحة جرائم مواقع التواصل الاجتماعي؟"**، وتتفرع عن هذه الإشكالية تساؤلات فرعية تتمثل في الآتي:

- ✓ ما موقع جرائم مواقع التواصل الاجتماعي في التشريع المغربي؟
- ✓ ما مدى ملاءمة النصوص الجنائية الحالية مع خصوصيات الجريمة المرتكبة عبر هذه الوسائل؟
- ✓ أين تتجلى مظاهر القوة والضعف في القانون المغربي في مواجهة هذه الجرائم؟

أولا-واقع جرائم مواقع التواصل الاجتماع في التشريع المغربي:

التشريع مقياس حقيقي للتقدم والرقي، وفن تحقيق العدالة والإنصاف، بل إن غايته الأساسية في المجتمع المعاصر لا تقف عند هذا الحد، وإنما تتجاوز ذلك إلى توجيه الجهود وتكريسها لتحقيق التقدم الاقتصادي والاجتماعي، وكفالة حقوق الإنسان في شموليتها. (الفاخوري، 2000)

ولعل القانون الجنائي من أهم مجالات التشريع التي يجب أن تستحضر فيها تلك المقاصد، والذي يجب أن يحظى بالاهتمام اللائق، وبدوام الإصلاح ليستوعب دوام التغيرات والتطورات المجتمعية، وفي المقابل يجب أن تكون الإصلاحات خاضعة لقواعد في الصياغة التشريعية ثابتة ومستقرة ومتفق عليها، وتهيمن على الأحكام التفصيلية وتتحكم فيها، وتضمن حكامة وجودة النصوص، في إنشائها أو في إصلاحها، وحتى في تطبيقها. (قاسمي، 2020)

وإذا كان تطور القانون الجنائي هو في نهاية المطاف تقنين لرد فعل المجتمع ضد أي سلوك معادي لكيانه، (الإدريسي، 2020) فإننا عندما نتكلم عن هذا التطور لا بد من استحضار مبدأ الشرعية الجنائية الذي ترتكز عليه

مجمل القوانين العقابية الوطنية والاتفاقيات الدولية لحماية حقوق الانسان والحريات الأساسية، بالإضافة إلى مبدأ التفسير الضيق للقانون الجنائي، الذي يشكل امتدادا طبيعيا لمبدأ شرعية الجرائم والعقوبات.

هذا، وفي خضم التزايد المضطرد في ظاهرة جرائم تقنية المعلومات الحديثة في العقدين الأخيرين، وبظهور طوفان الشبكة المعلوماتية وتوفير انسيابية لمرور البيانات عبر قنواتها في ظل هذه الصحوة الرقمية، تنامت حدة المخاطر المحدقة بالأشخاص والجرائم الواقعة على الأموال، وأضحت شبكات ومواقع التواصل الاجتماعي محل تقنين ومراقبة، إما مشددة أو مرنة، وهي مراقبة تصطدم بمبدأ أساسي من حقوق الإنسان، أي بحرية التعبير، وهو مبدأ يمتد ليشمل شبكة الأنترنت ومنصات التواصل الاجتماعي.

وكما هو الحال في جميع الدول، فقد عرف المغرب انتشار واستفحال جرائم تقنية المعلومات الحديثة، لكنه بخلاف مجموعة من الدول تأخر تضمين تشريعه الجنائي مقتضيات تتصدى لهذا الصنف من الإجرام المستحدث، مما دعا الفقه (عثماني، 2014) إلى المطالبة بضرورة سن قانون يهم جرائم تقنية المعلومات الحديثة بمختلف أصنافها. غير أن المشرع اختار مسلكا آخر معاكس لما طالب به الفقه، مسلك قوامه سن قوانين خاصة مشتتة في الزمان، بعض من هذه القوانين أدمج بمجموعة القانون الجنائي 5، في حين ألحقت النصوص الأخرى بقوانين مرتبطة بما هو إلكتروني.

1. ماهية جرائم مواقع التواصل الاجتماعي:

إذا كانت الجريمة طبقا للفصل 110 من القانون الجنائي هي: "عمل أو امتناع مخالف للقانون الجنائي"، فإن الملاحظ أن هذا التعريف لا يشتمل إلا على الركنين القانوني والمادي دون الركن المعنوي، وهو ما تداركه الفقه عند تعريفه للجريمة بأنها: "كل فعل أو امتناع صادر عن شخص قادر على التمييز يحدث اضطرابا اجتماعيا يعاقب عليه التشريع **الجنائي"**. (أبو العلاء، 2015)

وعليه، فالمشرع المغربي لم يعرف الجريمة الإلكترونية وإنما يستعمل هذا المصطلح للدلالة على كل نشاط إجرامي تكون فيه التقنيات التكنولوجيا والرقمية جزءا منه، إما باعتبار التكنولوجيا هدفا لذلك النشاط الإجرامي أو بكونها هي الوسيلة لتحقيق الجريمة.

وهكذا، نجد تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين يعرف الجريمة الإلكترونية بأنها: "كل جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية أو داخل نظام حاسوبي". (مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين، 10-2000/17)

أما خبراء منطقة التعاون الاقتصادي والتنمية في سنة 1983، عرفوا الجريمة الإلكترونية بأنها: "كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات". (نائلة، 2004)

وبناء على ذلك يمكن تعريف الجريمة الإلكترونية هي: "كل فعل أو عمل صادر عن شخص يتم بواسطة الأنظمة المعلوماتية عن قصد ونية إلحاق الضرر بالآخرين".

وانطلاقا مما سبق، يمكن القول إنه بالرغم من أن مجموعة من البلدان حاولت إصدار تشريعات تتعلق بمكافحة الجريمة الإلكترونية ومنها المغرب، إلا أن طابعها العام يتسم بعدم قدرتها على الإحاطة بكافة أشكال الإجرام المعلوماتي المتجدد والمتطور بشكل دائم، ويبقى الفراغ الذي يتركه عدم الإحاطة هذا فرصة لمجرمي هذا الصنف المستحدث من الجرائم لتنظيم أنفسهم، مما يستلزم تظافر الجهود الدولية لمواجهتها.

2. واقع جرائم منصات التواصل الاجتماعي في التشريع المغربي:

وعيا من المشرع المغربي بخصوصية الإجرام الإلكتروني وآثاره على المجتمع عمل منذ صدور القانون المتعلق بالإرهاب، الذي تضمن إمكانية ارتكاب الجريمة الإرهابية عن طريق نظم المعالجة الآلية للمعطيات، علما أن القانون الجنائي المغربي لا يحتوي على نصوص تخص الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، مما جعل المشرع يسن قانونا خاصا بهذا النوع من الجرائم من خلال القانون رقم 03.07 المتمم لمجموعة القانون الجنائي، فضلا عن وجود بعض المقتضيات القانونية المؤطرة لهذه الجرائم في القانون المتعلق بحقوق المؤلف والحقوق المجاورة.

وتتجلى صور الاعتداء على نظام المعالجة الآلية للمعطيات في الدخول أو البقاء غير المشروع في النظام، وعرقلة سير النظام وإحداث خلل فيه، ثم الإعداد لارتكاب المس بالنظام (الفصول من 607-3 إلى 607-11 من القانون الجنائي).

كما نجد أن المشرع المغربي تنبه لخطورة انتشار الإجرام المعلوماتي وأثر ذلك على أمن واستقرار المجتمع المغربي، وقد ظهر ذلك مع عرض مشروع القانون المتعلق بالإرهاب على مجلس الوزراء بتاريخ 16 يناير2003، حيث وردت لأول مرة الإشارة إلى إمكانية ارتكاب أفعال إجرامية إرهابية عن طريق المعالجة الآلية للمعطيات.

وما يلفت النظر هو أن القانون المغربي رقم03-03 المتعلق بالإرهاب يعد أول تشريع مغربي يشير بشكل صريح للإجرام المعلوماتي كوسيلة للقيام بأفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي يهدف إلى المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف، فالفصل 218-1 حدد بعض الأفعال المجرمة على سبيل الحصر، من بينها الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات (الفقرة 7)، وذلك بعد محاولة تحديد مفهوم الإرهاب في مستهل هذا الفصل. (الفوركي، 2020)

وباستقراء القانون المغربي المتعلق بمكافحة الإرهاب نستشف أن المشرع عاقب من خلال الفقرة 8 من الفصل 218-1 (ينص الفصل 218-1 من القانون الجنائي على أنه: "تعتبر الجرائم التالية أفعال إرهابية....8-تزوير أو تزييف الشيكات أو أي وسيلة أداء أخرى المشار إليها على التواليفي المادتين 316 و331 من مدونة التجارة...") على كل تزوير أو تزييف للشيكات أو أي وسيلة أداء أخرى تمت الإشارة إليها في المادتين 316و331 من مدونة التجارة المغربية. وبرجوعنا للمادة 331 من المدونة المذكورة نجدها متعلقة بموضوع الدراسة، بحيث فرضت العقوبات المنصوص عليها في المادة 316 في حالة تزوير أو تزييف وسيلة أداء، أو استعمالها أو محاولة ذلك، وحتى قبول الأداء-عن علم-بوسيلة أداء مزيفة أو مزورة. وبطبيعة الحال يدخل ضمن وسائل الأداء المشار إليها وسائل الأداء الحديثة مثل بطاقات الدفع الالكتروني.

ومما تجدر الإشارة إليه عند الحديث عن القانون المغربي رقم 03-03 المتعلق بمكافحة الإرهاب أن الفصل 2-218 منه عاقب على استعمال وسائل الإعلام ومنها الالكترونية في الإشادة بالأعمال الإرهابية، وقد حدد الفصل المذكور العقوبة في الحبس من سنتين الى ست سنوات وبغرامة بين 10 آلاف و200 ألف درهم. ومعلوم أن وسائل الإعلام الالكترونية متعددة من أبرزها الشبكة الدولية للمعلومات-الانترنت-.

وينضاف إلى هذه القوانين المقتضيات الزجرية الواردة في كل من القانون رقم 09.09 المتعلق بحماية الأشخاص الذاتيين تجاه المعالجة الآلية للمعطيات، والقانون رقم 53.05 المتعلق بالتبادل الإلكتروني للمعطيات القانونية.

فبعد أن أصبحت البيانات الشخصية المعالجة الكترونيا ذات أهمية على المستوى الدولي، وهذا ما جعل الأمم المتحدة تتبنى عام 1989 دليلا يتعلق باستخدام الحوسبة في عملية تدفق البيانات الشخصية، وبتاريخ 1990/12/14، تبنت الهيئة العامة دليل تنظيم استخدام المعالجة الآلية للبيانات الشخصية. (GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES. Adopted by the General Assembly, 14 december 1990) (Francesco , 2000)

وقد سار المشرع المغربي مع التوجه التشريعي في العديد من الدول التي تهدف تحقيق حماية فعالة للبيانات الشخصية، فأصدر القانون رقم 08-09 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي بتاريخ 18 فبراير 2009، (منشور بالجريدة الرسمية عدد 5700 بتاريخ 23 فبراير 2009) ويتضمن هذا التشريع 51 مادة موزعة على ثمانية أبواب. وتبدو أهمية هذا القانون في كونه سيساهم في تقوية ثقة المستهلك المغربي في المعاملات الالكترونية والاستفادة من مزايا التجارة الالكترونية، وسيشكل هذا التشريع كذلك أداة هامة لحماية الحياة الخاصة والبيانات الشخصية للمواطن المغربي خصوصا في مجال المعلوميات، وقد أوضح المشرع ذلك صراحة في مستهل المادة الأولى من هذا القانون، بحيث تنص المادة الأولى: "المعلوميات في خدمة المواطن وتتطور في إطار التعاون الدولي. ويجب ألا تمس بالهوية والحقوق والحريات الجماعية أو الفردية للإنسان. وينبغي ألا تكون أداة لإفشاء أسرار الحياة الخاصة للمواطنين............"

وما يهمنا ضمن القانون المغربي رقم 08-09 هو الباب السابع الخاص بالعقوبات، والذي جاء بمجموعة من النصوص التي تحمي عمليات المعالجة وتحمي المعطيات الشخصية المعالجة، ومن أهم المواد نجد المادة 53 التي عاقبت بالغرامة من 20000درهم إلى 200000 درهم في حالة رفض المسؤول عن المعالجة حقوق الولوج أو التصريح أو التعرض المنصوص عليها في المواد 7 و8 و9 من القانون رقم 08 -09.

كما جرمت المادة 63 عملية نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43و44 من هذا القانون. (تنص المادة 60 على أنه: "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20000 درهم إلى 200000 درهم أو بإحدى هاتين العقوبتين فقط كل من نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43 و44 من هذا القانون.")

كما نجد هذا التشريع الجديد تطرق للحالات التي تؤدي للاستعمال التعسفي أو التدليسي للمعطيات المعالجة أو إيصالها لأغيار غير مؤهلين من طرف المسؤول عن المعالجة او كل معالج من الباطن أو كل شخص مكلف-بفعل مهامه-بمعالجة معطيات ذات طابع شخصي، وقد حددت العقوبة من 6 أشهر إلى سنة وبغرامة من ألف درهم إلى 300 ألف درهم. (المادة 61 من القانون 09.08)

أما المادة 63 فقد عاقبت كل مسؤول عن المعالجة في حالة رفضه تطبيق قرارات_اللجنة الوطنية، المذكورة سلفا، والتي أحدثها القانون المغربي رقم 08-09.

وتجدر الإشارة إلى انه وفق التشريع المذكور تضاعف عقوبات الغرامة الواردة في نصوص هذا التشريع إذا كان مرتكب إحدى المخالفات شخصا معنويا، دون المساس بالعقوبات التي قد تطبق على المسيرين. مع إمكانية معاقبة الشخص المعنوي بالمصادرة والإغلاق.

أما بخصوص القانون رقم 05-53 فإنه إذا كان قد أثر بشكل أساسي على فصول قانون الالتزامات والعقود المغربي بفعل تعديل بعض نصوصه أو إضافة أخرى جديدة متصلة بالبيئة المعلوماتية، إلا انه يتضمن كذلك مجموعة من النصوص الزجرية، والتي تساهم في مكافحة الجرائم المعلوماتية، نذكر منها المادة 29 التي تعاقب كل من يقدم خدمات للمصادقة الالكترونية المؤمنة خلافا للمادة 20 أو دون أن يكون معتمدا أو من يواصل نشاطه رغم سحب اعتماده.

كذلك المادة 31 فتعاقب على الإدلاء العمدي بتصاريح كاذبة أو تسليم وثائق مزورة إلى مقدم خدمات المصادقة الالكترونية.

ومن أجل ضمان سلامة تبادل المعطيات القانونية بطريقة الكترونية وضمان سريتها وصحتها، فرض المشرع حماية خاصة لوسائل التشفير من خلال المادة 32 التي تجرم استيراد أو استغلال أو استعمال إحدى الوسائل أو خدمة من خدمات التشفير دون الإدلاء بالتصريح أو الحصول على الترخيص، كما انه يمكن للمحكمة الحكم بمصادرة وسائل التشفير المعنية. (تنص المادة 32 على أنه: "يعاقب بالحبس لمدة سنة وبغرامة مبلغها100000 درهم كل من استورد أو صدر أو ورد أو استغل أو استعمل إحدى الوسائل أو خدمة من خدمات تشفير دون الإدلاء بالتصريح أو الحصول على الترخيص المنصوص عليهما في المادتين13و14اعلاه".)

كما جرم المشرع المغربي كل استعمال لوسيلة تشفير لتمهيد أو ارتكاب جناية أو جنحة أو لتسهيل تمهيدها أو ارتكابها لكن ذلك لا يطبق على مرتكب الجريمة أو المشارك في ارتكابها الذي يسلم إلى السلطات القضائية أو الإدارية، بطلب منها، النص الواضح للرسائل المشفرة وكل ما يلزم لقراءة النص المشفر.

ولتحقيق حماية جنائية للتوقيع الالكتروني عاقبت المادة 35 كل استعمال غير قانوني للعناصر الشخصية لإنشاء التوقيع المتعلقة بتوقيع الغير.

كما حمى المشرع المغربي، من خلال المادة 37، حجية الشهادة الالكترونية عبر تجريم الاستمرار في استعمالها بعد مدة صلاحيتها أو بعد إلغائها.

وتجدر الإشارة إلى أن الغرامات -المنصوص عليها في هذا القانون-ترفع إلى الضعف، إذا كان مرتكب الجريمة شخصا معنويا، دون الإخلال بالعقوبات الممكن تطبيقها على المسيرين لارتكاب إحدى الجرائم المذكورة في هذا القانون. كما يمكن أن يتعرض الشخص المعنوي لعقوبات أخرى تتجلى في المصادرة أو الإغلاق.

أما فيما يتعلق بالقانون رقم 34.05 المعدل والمتمم للقانون رقم 02.00 المتعلق بحقوق المؤلف والحقوق المجاورة، تم وضع مقتضيات جنائية خاصة في القانون المتعلق بحقوق المؤلف، ومن بينها ما جاءت به المادة 64 التي عاقبت بالحبس من شهرين إلى 6 أشهر وغرامة من 10000 درهم إلى 100000 درهم أو بإحدى هاتين العقوبتين فقط لكل من قام بطريقة غير مشروعة بقصد الاستغلال التجاري بخرق متعمد، كما تطبق نفس العقوبة على أفعال استيراد وتصدير نسخ منجزة خرقا للقانون وعدة أعمال ينص عليها القانون وبالأخص ما له علاقة بالتكنولوجيا الحديثة.

وتضاعف العقوبة في حالة الاعتياد على ارتكاب المخالفة، وترفع العقوبة الحبسية لما يتراوح بين سنة وأربع سنوات وغرامة ما بين 60000درهمو600000درهم أو بإحدى هاتين العقوبتين في حالة العود داخل خمس سنوات بعد صدور حكم نهائي.

وقد جاء التعديل الجديد بتدابير وقائية وعقوبات إضافية تتجلى في خمسة.

1. حجز النسخ والأدوات وكذا الوثائق والحسابات والأوراق الإدارية المتعلقة بهذه النسخ
2. مصادرة جميع الأصول متى ثبت علاقتها بالنشاط غير القانوني.
3. إتلاف النسخ والأدوات المستعملة من اجل إنجازها.
4. الإغلاق النهائي أو المؤقت للمؤسسة التي يستغلها مرتكب المخالفة او شركاؤه فيها.
5. نشر الحكم القاضي بالإدانة في جريدة أو أكثر، يتم تحديدها من طرف المحكمة المختصة.

وبعد ذكرنا لأهم القوانين التي تحكم الأفعال الإجرامية المشكلة للجرائم الإلكترونية يبقى لنا أن نتساءل عن مدى استيعاب هذه القوانين لمختلف الجرائم التي اتخذت مواقع التواصل الاجتماعي فضاء لها وأداة لإنتاج أنشطة تهدد مرتاديها؟

فبالرجوع إلى القانون 03.07 المتعلق بالمس بنظم المعالجة الآلية للمعطيات يتضح لنا أن المشرع لم يعرف الجريمة المعلوماتية أو الإلكترونية، واقتصر على بيان أوجه الأفعال غير المشروع التي تمثل انتهاكا لهذه النظم والعقوبات المقررة لها، الأمر الذي جعل القضاء المغربي يحاول البحث عن مبدأ الشرعية الجنائية في نصوص أخرى غير هذا النص، فبالنسبة لجريمتي السب والقذف العلني والتشهير يتم الاستناد على قانون الصحافة والنشر رقم 88.13، بالنظر إلى كون المشرع رغم نصه على هذه الجرائم ضمن مجموعة القانون الجنائي إلى أنه من حيث العقوبة أحال على قانون الصحافة والنشر. فضلا عن أن القضاء يجد نفسه مطالبا بما يملك من سلطة تقديرية أن يتعامل مع جرائم تقع في

الواقع وتقع تحت طائلة القانون الجنائي لكن لها امتدادات على مواقع التواصل الاجتماعي، كنشر فيديوهات الإيذاء المبهج على صفحات الفيسبوك والتطبيقات الأخرى، ومن أمثلة ذلك اغتصاب فتاة الراشيدية بالحافلة، وفيديو الزوجة التي عرضها زوجها لمحاولة القتل بالشارع العام بمدينة سيدي قاسم، وظاهر تصوير واستعراض الأسلحة البيضاء أو ما يعرف ب "التشرميل". مما يمكن معه القول أن المشرع مدعو إلى إعادة النظر في نصوصه الجنائية ومحاملة ملاءمتها مع خصوصيات الإجرام الإلكتروني الجديدة والمتطورة باستمرار، وهو ما حاول القيام به من خلال مشروع القانون رقم 22.20 المتعلق باستعمال مواقع التواصل الاجتماعي، الذي سيكون موضوع النقطة الموالية.

ثانيا-قراءة في مشروع القانون رقم 22.20 المتعلق باستعمال مواقع التواصل الاجتماعي:

تجدر الإشارة بداية إلى أن نصوص هذا القانون ليست وحدها التي تطبق على هذا المجال، حيث أن المشرع المغربي لحظة شعوره بخطورة الجريمة الإلكترونية، منذ بداية القرن الحادي والعشرين، أوجد حينها في صلب القانون الجنائي باباً خاصاً يتعلق بالمس بنظم المعالجة الآلية للمعطيات منذ سنة 2003، إلا أن سرعة تطور تكنولوجيا المعلومات، أدت إلى شيوع استعمال هذه الوسيلة في ارتكاب جرائم متعددة ومختلفة يمتد أثرها خارج الحدود الوطنية والإقليمية. كما أن المشرع قد استحضر في هذا السياق روح الاتفاقية الأوروبية حول الإجرام المعلوماتي، إبان وضعه للباب العاشر من الجزء الأول من الكتاب الثالث من مجموعة القانون الجنائي (المواد 3-607 إلى 11-607، ومن ثم، فإن المستجدات الحاصلة في مجال استخدام المعلومات في ارتكاب الجرائم العابرة للحدود، جعلت الدولة المغربية تصادق على اتفاقية "بودابست" حول الجريمة المعلوماتية.

كما نجد القانون 103.13 تضمن مقتضيات جديدة تتعلق بحماية الحياة الخاصة للأفراد، التي سبق إقرارها دستوريا بموجب الفصل 24 من الدستور، على اعتبار أن تلك النصوص رغم ورودها ضمن قانون محاربة العنف ضد النساء، فإنها جاءت بمقتضيات تكتسي صبغة عامة، أي أنها تطبق بغض النظر عن جنس الضحايا ذكورا كانوا أم إناثا. وبموجب ذلك، تم إدخال تعديلات على المدونة الجنائية، حيث أن الفصل 447-2من ق.ج ينص على أنه: "يعاقب بالحبس من سنة واحدة إلى ثلاث سنوات وغرامة من 2.000 إلى 20.000 درهم، كل من قام بأي وسيلة بما في ذلك الأنظمة المعلوماتية، ببث أو توزيع تركيبة مكونة من أقوال شخص أو صورته، دون موافقته، أو قام ببث أو توزيع ادعاءات أو وقائع كاذبة، بقصد المس بالحياة الخاصة للأشخاص أو التشهير بهم". وحسب المادة 3-447 من ق.ج ترتفع هذه العقوبة لتبدأ بالحبس من سنة واحدة إلى خمس سنوات وغرامة من 5.000 إلى 50.000 درهم، في حالة ارتكابها من طرف الزوج أو الطليق أو الخاطب أو أحد الأصول أو الكافل أو شخص له ولاية أو سلطة على الضحية أو مكلف برعايتها أو ضد امرأة بسبب جنسها أو ضد قاصر. وفي نفس السياق سبق لرئيس النيابة العامة أن وجه تعليماته إلى المحامي العام الأول لدى محكمة النقض وللوكلاء العامين للملك لدى محاكم الاستئناف ووكلاء الملك لدى المحاكم الابتدائية من أجل السهر على التطبيق الصارم للقانون بشأن حماية الحياة الخاصة للأفراد في ظل القانون رقم 103.13 المتعلق بمحاربة العنف ضد النساء. (منشور عدد: 48 س/ ر ن ع حول حماية الحياة الخاصة للأفراد في ظل القانون رقم 103.13، بتاريخ 06 ديسمبر 2018)

في ظل الأجواء الصحية التي عاشها المغرب ولا يزال جراء انتشار كوفيد 19، وما نتج عنه من اتخاذ الدولة لعدة إجراءات استباقية لازمة لمواجهة هذه الجائحة، وبالموازاة مع ذلك نجد بعض السلوكيات غير القانونية التي تتم عبر مواقع التواصل الاجتماعي عن طريق نشر أخبار وحقائق زائفة وتضليلية حول معطيات ومعلومات مغلوطة وكاذبة تحمل الاسم والصفة حول إصابة شخص بهذا الفيروس دون إصابته بذلك في الحقيقة، وكذا نشر فيديوهات عبر قنوات اليوتيوب حول عدم وجود هذا الفيروس، إضافة إلى فبركة بلاغات مختلف الوزارات ونسبها للجهات الرسمية وأنها صادرة عنهم وفي الحقيقة لا علاقة لها بالجهة المصدرة للخبر، فالغاية من هذا كله هو نشر الخوف إثارة البلبلة بين الناس، وأيضا كسب الإعجاب (الليكات) رفع نسب المشاهدة، غير مكترثين بما تحدثه هذه السلوكيات ومثيلتها من اضطراب اجتماعي وأنها تقع الجنائي تحت طائلة العقاب. (الفصل الثاني من القانون الجنائي الذي جاء فيه: "لا يسوغ لأحد أن يعتذر بجهل التشريع الجنائي".)

وأمام هذا الخطر المستحدث والواسع النطاق، والذي صادف ظرفية صعبة يمر منها المغرب كغيره من الدول تم تمرير ومصادقة الحكومة على مشروع القانون رقم 22.20 يتعلق باستعمال مواقع التواصل الاجتماعي وشبكات البث المفتوحة والشبكات المماثلة، هذا المشروع الذي جاء في إطار التوفيق بين التدابير التشريعية والمؤسساتية التي تنهجها الدولة لمكافحة الإجرام الإلكتروني والحق في التواصل الرقمي باعتباره صورة من صور حرية التعبير المكفولة دستوريا. كما يهدف مشروع القانون هذا إلى سد الفراغ التشريعي الذي تعرفه المنظومة القانونية الوطنية لردع الاستخدامات غير المشروعة لمواقع التواصل الاجتماعي، فضلا عن ملاءمة التشريع الداخلي مع الالتزامات الدولية للمملكة، وعلى رأسها اتفاقية بودابست المتعلقة بالجرائم الإلكترونية، التي صادق عليها المغرب بتاريخ 29 يونيو 2018.

ويتضح من خلال القراءة الشكلية لمقتضيات مشروع هذا القانون، أنه يتضمن 25 مادة موزعة على ثلاثة أبواب، حيث خصص الباب الأول منه للتعريف ببعض المصطلحات الآتية: شبكة التواصل، شبكات البث المفتوح، البيانات، المحتوى الإلكتروني، الهوية الرقمية، حرية التواصل الرقمي عبر شبكات التواصل الاجتماعي. بالإضافة إلى بيان نطاق سريان أحكامه ومجال تطبيقه)المواد من 1 إلى 4). وفي الباب الثاني فقد تعرض لنظام تزويد خدمات شبكات التواصل الاجتماعي وشبكات البث المفتوح والشبكات المماثلة، سواء من حيث جهة الإشراف والرقابة، أو من جانب الالتزامات الواقعة على عاتق مزودي الخدمات، بالإضافة إلى الجزاءات الإدارية (المواد من 5 إلى 12). أما باقي المواد فقد ضمنها في باب ثالث خاص بالمقتضيات الزجرية (المواد من 13 إلى 25)، حيث صنف الجرائم بحسب الطبيعة إلى أربعة أنواع: الجرائم الماسة بالأمن والنظام العام الاقتصادي (المواد من 13 إلى 15)، جرائم نشر الأخبار الزائفة (المواد من 16 إلى 19)، جرائم الماسة بالشرف والاعتبار الشخصي (المواد من 20 إلى (22، ثم خصص المواد من 23 إلى 25 من نفس المشروع للجرائم الواقعة على القاصرين دون سن 18 سنة وذوي العاهات، باعتبارهم –في نظرنا-الفئة الأولى بالحماية.

وقد أثار مشروع القانون رقم 22.20 نقاشا قانونيا وسياسيا كبيرا، ووجهت بعض مقتضياته بمعارضة من طرف المجتمع المغربي بكل فئاته وبانتقاد من مختلف المهتمين بالشأن الحقوقي والقانوني ببلادنا، وهمت تلك الانتقادات التي

لقيها هذا المشروع من جهة المسطرة التي جرى بموجبها اعتماد هذا النص من طرف الحكومة، ومن جهة أخرى المقتضيات التي تضمنتها بعض مواده وما تثيره تلك المقتضيات من مس وتضييق على الحقوق والحريات التي يكفلها الدستور المغربي لكافة المواطنين.

وبعيدا عن الجدال السياسي الذي أثاره هذا المشروع بين مختلف الأحزاب والهيئات السياسية، سنحاول التوقف عند ما يثيره هذا المشروع من إشكالات دستورية وقانونية.

1. **ملاحظات في مسطرة الإعداد والمصادقة:**

أثارت الطريقة التي جرى بها اعداد واعتماد الحكومة مشروع القانون رقم 22.20 عدة ملاحظات، تهم أساسا مخالفتها للقواعد التي نص عليها دستور سنة 2011 وكذا للإجراءات التي تأطر العمل الحكومي في مجال المسطرة التشريعية المنظمة من خلال مختلف النصوص القانونية والتنظيمية ذات الصلة.

حيث أن الحكومة ممثلة في وزارة العدل، لم تحترم في إعدادها لهذا المشروع مبدأ الديمقراطية التشاركية الذي نص عليه الدستور في فصله الأول والذي اعتبره كأحد مقومات النظام الدستوري للمملكة. (الأشكورة، 2020)

فالدستور وإن منح لرئيس الحكومة بموجب الفصل 78 حق اقتراح القوانين، فإنه ألزم الحكومة بإعمال مبدأ الديمقراطية التشاركية قبل عرض أي مشروع قانون على مسطرة المداولة والمصادقة، بغية أخذ آراء ومقترحات الهيئات الدستورية والوطنية ومختلف الفاعلين والمهتمين وعموم المواطنين، خاصة إذا تعلق الأمر بنص ينظم مجالا ذا أبعاد متعددة مثل شبكات التواصل الاجتماعي وشبكات البث المفتوح والذي يرتبط بممارسة أحد الحقوق والحريات الأساسية التي يكفلها الدستور والذي هو الحق في حرية التعبير. (ريحي، 2020)

والواضح أن الحكومة غيبت في إعدادها لهذا النص تفعيل مبدأ الديمقراطية التشاركية، حيث كان من المفترض على وزارة العدل قبل عرضه على المجلس الحكومي، أن تفتح مشاورات موسعة حول مضامينه وأن تعمل على أخذ آراء الهيئات الدستورية والمدنية المعنية بحماية والدفاع عن حقوق الإنسان والحريات الأساسية، وأخص بالذكر هنا المجلس الوطني لحقوق الإنسان الذي أناط به الدستور في فصله 161 مهمة النظر في جميع القضايا المتعلقة بالدفاع عن حقوق الإنسان والحريات وحمايتها، وبضمان ممارستها الكاملة، والنهوض بها.

وهذا الأمر الذي حاولت وزارة العدل تداركه من خلال بيان وزير العدل الذي قال فيه أنه سيطلب من رئيس الحكومة ومن أعضاء اللجنة الوزارية المكلفة بمراجعة هذا المشروع تأجيل أشغال هذه الأخيرة، وفتح مشاورات موسعة حول مضامين القانون المذكور مع مختلف الهيئات المعنية.

وإضافة إلى ما سبق، تطرح الصيغة التي حملها بيان الحكومة الصادر عقب اجتماعها المنعقد بتاريخ 19 مارس 2020 ملاحظة مسطرية أخرى. حيث جاء فيه أن المجلس الحكومي تدارس وصادق على مشروع قانون رقم 22.20 يتعلق باستعمال شبكات التواصل الاجتماعي وشبكات البث المفتوح والشبكات المماثلة، قدمه السيد وزير العدل، مع

الأخذ بعين الاعتبار الملاحظات المثارة في شأنه بعد دراستها من طرف اللجنة التقنية ثم اللجنة الوزارية المحدثتين لهذا الغرض.

فالمجلس الحكومي إذن قام بمدارسة النص المذكور والمصادقة عليه مع تشكيل لجنتين تقنية ووزارية لمدارسة الملاحظات المثارة بشأنه، وهو أمر مخالف للإجراءات الشكلية التي تنظم العمل الحكومي في مجال التشريع. (الأشكورة، 2020)

فبالرجوع إلى القانون التنظيمي رقم 65.13 المتعلق بتنظيم وتسيير أشغال الحكومة والوضع القانوني لأعضائها، لاسيما من المادة 19 إلى المادة 23 المتعلقة بمشاريع النصوص القانونية المعروضة على مسطرة المصادقة، وبالعودة إلى دليل المساطر التشريعية والتنظيمية الذي أعدته وأصدرته وزارة العلاقات مع البرلمان تطبيقا للمادة 20 من القانون التنظيمي سالف الذكر يلاحظ أنها خرقت هذه القواعد.

فالحكومة كان عليها أن تؤجل المصادقة على مشروع هذا النص إلى حين حسم اللجنتين التقنية والوزارية في الملاحظات التي تطرحها مقتضياته، وليس العكس، فالصيغة التي اعتمدتها الحكومة تفرض ضرورة إعادة النص إلى المجلس الحكومي بعد انتهاء اللجنتين المحدثتين بغية البث في صيغته النهائية، وهذا ما يساءل الجدوى من المصادقة عليه في المرة الأولى.

وهذه الملاحظات المسطرية تجعلنا نتساءل عن الأداء التشريعي للحكومة خاصة إذا أضفنا إليها غياب مخطط تشريعي يحدد الأولويات الحكومية بشكل واضح ومنسجم.

2. **ملاحظات بشأن بعض مقتضيات المشروع:**

أثارت المقتضيات التي جاء بها مشروع القانون 22.20 نقاشا حقوقيا وقانونيا كبيرا وعميقا بين مختلف شرائح المجتمع المغربي ولا سيما المهتمين بالشأن الحقوقي والقانوني، وتستند الانتقادات الموجهة إلى مضامينه على ما تضمنه بصفة خاصة الفصل الأول من الباب الثالث والمتعلق بالجرائم الماسة بالأمن والنظام العام الاقتصادي لاسيما المادتين 14 و15.

حيث تنص المادة 14 على تجريم استعمال شبكات التواصل الاجتماعي أو شبكات البث المفتوح أو الشبكات المماثلة في الدعوة إلى مقاطعة بعض المنتوجات أو البضائع أو الخدمات أو القيام بالتحريض على ذلك، وعاقبت من قام عمدا بهته الأعمال بعقوبة حبسية بين ستة أشهر وثلاث سنوات وبغرامة مالية بين 5000 و50000 درهم أو بإحدى هتين العقوبتين، ونفس الجزاء نصت عليه المادة 15 بالنسبة لكل من قام عمدا بحمل العموم أو تحريضهم عبر هاته الوسائط على سحب الأموال من مؤسسات الائتمان أو الهيئات المعتبرة في حكمها.

إن ما نصت عليه المادتين السالفتين سيشكل في حالة اعتمادهما بالصيغة التي جاء بها المشروع تراجعن عن المكتسبات الكبيرة التي حققتها بلادنا في مجال حماية حقوق الإنسان، ومسا خطيرا بحرية التعبير والرأي والتفكير التي يكفلها الدستور المغربي والمواثيق الدولية التي صادقت عليها بلادنا. (التايب، 2020)

فقد يصبح أي تعبير للأشخاص عبر هذه الشبكات عن آرائهم بخصوص منتوج أو بضاعة أو خدمة ما، سببا في تعرضهم لعقوبات ثقيلة، وهو أمر يتعارض في رأينا مع أحكام الدستور لاسيما صريح الفصل 25 منه والذي ينص على أن حرية الفكر والرأي والتعبير مكفولة بكل أشكالها.

فالمشرع الدستوري حين كفل للجميع حرية ممارسة الحق في التعبير والرأي والتفكير، لم يقيد هذا الحق بأية قيود، كما أنه لم يربط ممارسته بأي شرط مثل ما هو عليه الحال بالنسبة لبعض الحقوق التي ربط ممارستها بصدور قانون ينظمها كالحق في الحصول على المعلومة أو الحق في التنقل عبر التراب الوطني الذي ضمنه وفقا للقانون.

ولذلك فإن أي تقييد للحق في التعبير والرأي والتفكير يبقى غير مشروع إلا في الحالات التي تتعارض فيها ممارسة هذا الحق مع حق آخر محمي بنص الدستور أو بأحد الحقوق المنصوص عليها في المعاهدات والاتفاقيات التي صادق عليها المغرب، وكمثال على هذه الحقوق التي قد تتعرض للانتهاك بممارسة حرية التعبير نذكر الحق في حماية الحياة الخاصة الفصل 24، أو حينما تستغل حرية التعبير في التحريض على العنصرية أو الكراهية أو العنف المحظور بموجب الفصل 23.

وفي نفس السياق، يمكن التوقف عند ما أشارت إليه المادة الثانية والتي جاء فيها أن حرية التواصل الرقمي عبر شبكات التواصل الاجتماعي وشبكات البث المفتوح وباقي الشبكات المماثلة مضمونة.

فالمشروع في هذه المادة نص على ضمان الحرية في التواصل فقط دون تأكيد على حرية التعبير والرأي، غير أن هذه الشبكات أصبحت اليوم فضاءات حاضنة للحريات والحقوق خاصة حرية التعبير، ولم تعد وظيفتها مقتصرة على مجرد التواصل بين الأفراد والجماعات.

بالإضافة إلى ما سلف أشارت وزارة العدل في تقديمها لهذا المشروع، أن إعداده جاء لسد الفراغ التشريعي الذي تعاني منه المنظومة القانونية الوطنية، ولملاءمة هذه المنظومة مع القوانين المقارنة والمعايير المعتمدة في مجال محاربة الجريمة الالكترونية، خاصة بعد مصادقة بلادنا على اتفاقية بودابيست المتعلقة بالجريمة المعلوماتية بتاريخ 29 يونيو 2018.

وبرجوعنا إلى اتفاقية بودابيست، لا نجدها متضمنة لأي مقتضى متعلق بالنظام العام الاقتصادي أو يجرم أي شكل من أشكال الدعوة إلى المقاطعة، وهي بالعكس من ذلك تأكد في ديباجتها على حرص الدول الأعضاء في هذه الاتفاقية على ضرورة تأمين التوازن الملائم بين المصالح المتصلة بإنفاذ القانون من جهة واحترام حقوق الإنسان الأساسية كما هو منصوص عليه في اتفاقية مجلس أوروبا لعام 1950 بشأن حماية حقوق الإنسان والحريات الأساسية، والعهد الدولي للأمم المتحدة لعام 1966المتعلق بالحقوق المدنية والسياسية، وغيرها من المعاهدات الدولية بشأن حقوق الإنسان السارية والتي تؤكد حق كل فرد في التعبير عن رأيه دون أي تدخل، وكذلك الحق في حرية التعبير، بما في ذلك حرية البحث عن مختلف أنواع المعلومات والأفكار وتلقيها ونقلها بغض النظر عن الحدود.

هذا التوازن بين ضمان إنفاذ القانون واحترام الحقوق والحريات الأساسية، في رأينا، مختل في الصيغة الحالية لمشروع القانون رقم 22.20 كما صادقت عليه الحكومة.

وإن إعلان الحكومة تأجيلها النظر في هذا المشروع أمر صائب بل ضروري في رأينا، إلى حين تجاوز بلادنا لهذه الظرفية الصحية الصعبة، مع الالتزام بفتح حوار وطني موسع مع مختلف المؤسسات والهيئات والمهتمين حول مضامينه، بما يمكن من ضمان ممارسة كل الحقوق والحريات الأساسية التي يكفلها الدستور لكافة المواطنين والمواطنات في نطاق التلازم بين ممارسة الحقوق بالنهوض بأداء الواجبات.

خاتمة:

إن ظاهرة الإجرام الإلكتروني على مواقع وتطبيقات التواصل الاجتماعي أصبحت نتيجة حتمية للتطور التكنولوجي، لذا فمواجهة هذا النوع الجديد من الإجرام لا يتحقق بتفسير النصوص التقليدية على اختلافها على نحو لا تحتمله، أو التوسع في إسقاط مفاهيم عن حالات أخرى قد تكون بعيدة عنها، لهذا يتعين على المشرع توسيع ترسانته القانونية وعدم الاقتصار على القواعد الجنائية العامة أو بعض النصوص القانونية الطارئة التي فرضتها بعض الظروف التي مرت بها المملكة، لأنها مع كل ما تحمله من مضامين إيجابية تبقى قاصرة عن مواكبة التطورات التكنولوجية والاكتساح الكبير للسلوكيات غير المشروعة على هذه المواقع، لذلك يمكن القول أنه ينبغي على المشرع إعادة النظر في مضامين القانون رقم 22.20 والأخذ بعين الاعتبار الانتقادات الحقوقية التي وجهت له، حتى يتسنى للمغرب أن يكون له قانون خاص بهذه المواقع والتطبيقات، يضمن الحريات ويحافظ على الحقوق ويقف سدا منيعا أمام كل التجاوزات.

قائمة المراجع:

1) (s.d.).

2) أبو العلاء، أ .(2015). *الجريمة من خلال علم الإجرام من حيث الأسباب والعلاج*. تطوان: مطبعة الخليج العربي.

3) إدريس الفاخوري. (2000). تطور القانون: الأسباب والوسائل. *مجلة المرافعة*(11)، 60.

4) إسماعيل الأشكورة. (13 أبريل، 2020). *قراءة دستورية في مشروع القانون رقم 22.00*. تم الاسترداد من جريدة السفير 24: https://assafir24.ma/83419/

5) الفصل الثاني من القانون الجنائي الذي جاء فيه: "لا يسوغ لأحد أن يعتذر بجهل التشريع الجنائي.(s.d.) ".

6) المادة 61 من القانون 09.08. (بلا تاريخ).

7) المادة 61 من هذا القانون. (بلا تاريخ).

8) تنص المادة 32 على أنه: "يعاقب بالحبس لمدة سنة وبغرامة مبلغها100000 درهم كل من استورد أو صدر أو ورد أو استغل أو استعمل إحدى الوسائل أو خدمة من خدمات تشفير دون الإدلاء بالتصريح أو الحصول على الترخيص المنصوص عليهما في المادتين13و14اعلاه.(s.d.) ".

9) تنص المادة 60 على أنه: "يعاقب بالحبس من 3 أشهر إلى سنة وبغرامة من 20000 درهم إلى 200000 درهم أو بإحدى هاتين العقوبتين فقط كل من نقل معطيات ذات طابع شخصي نحو دولة أجنبية خرقا لأحكام المادتين 43 و44 من هذا القانون". (بلا تاريخ).

10) خالد عثماني. (2014). مكافحة الجريمة الإلكترونية في ضوء التشريع المغربي. *مجلة العلوم الجنائية*(1)، 38.

11) مصطفى الفوركي. (2020). الجرائم الماسة بالنظم المعلوماتية في القانون المغربي. *مجلة البحوث القانونية والاقتصادية، 3*(1)، الصفحات 554-567.

12) منشور بالجريدة الرسمية عدد 5700 بتاريخ 23 فبراير 2009. (بلا تاريخ). 552.

13) منشور عدد: 48 س/ ر ن ع حول حماية الحياة الخاصة للأفراد في ظل القانون رقم 103.13) .بتاريخ 06 ديسمبر 2018 Récupéré sur .(موقع رئاسة النيابة العامة) :

https://www.pmp.ma/download/%d8%ad%d9%88%d9%84-%d8%ad%d9%85%d8%a7%d9%8a%d8%a9-%d8%a7%d9%84%d8%ad%d9%8a%d8%a7%d8%a9-%d8%a7%d9%84%d8%ae%d8%a7%d8%b5%d8%a9-%d9%84%d9%84%d8%a3%d9%81%d8%b1%d8%a7%d8%af-%d9%81%d9%8a-%d8%b8%d9%84-3/?wpdmdl=5208

14) مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين. (10-2000/17). فيينا.

15) مولاي عبد الرحمان قاسمي. (2020). قواعد في صياغة النص الجنائي كمدخل للإصلاح. *المجلة الدولية للأبحاث الجنائية والحكامة الأمنية*(3)، 478.

16) نائلة، ق .(2004). *جرائم الحاسب الاقتصادية*. القاهرة: دار النهضة العربية.

17) هشام العزوزي الإدريسي. (2020). مبدأ الشرعية الجنائية والتكنولوجيا الجديدة. *المجلة الدولية للأبحاث الجنائية والحكامة الأمنية*(3)، 285.

18) ينص الفصل 218-1 من القانون الجنائي على أنه: "تعتبر الجرائم التالية أفعال إرهابية....8-تزوير أو تزييف الشيكات أو أي وسيلة أداء أخرى المشار إليها على التواليفي المادتين 316 و331 من مدونة التجارة.(s.d.) "...

19) يوسف ريجي. (29 أبريل، 2020). *مقاربة التوجه التشريعي لمشروع القانون رقم 22.20 المتعلق باستعمال شبكات التواصل الاجتماعي: قراءة نقدية*. تم الاسترداد من موقع دروس القانون: https://www.coursdroitarab.com/2020/04/law-22.20.html

20) يونس التايب. (30 أبريل، 2020). *ملاحظات أولية حول مسودة مشروع القانون رقم 22.20*. تم الاسترداد من موقع دكالة tv: https://doukkala.tv/?p=7097

21) francesco , m. (2000). le cadre réglementaire des traitments de donné personnelles effectues au sien de l'unioneuropéenne. revue trimestrielle de droit européen(2), p. 283.

22) guidelines concerning computerized personal data files. adopted by the general assembly. (14 december 1990).

التعاون الإقليمي الأوروبي في مواجهة الجريمة الالكترونية
اتفاقية بودابست نموذجا

European regional cooperation against crime Electronic
Budapest Convention as a model

د.أمال بن صويلح/ جامعة قالمة/ الجزائر
Dr.Amel bensouilah/ University of Guelma/ Algeria

ملخص الدراسة:

تعد الجريمة الالكترونية من أخطر الجرائم التي تواجهها أنظمة الحماية خصوصا والدول اجمالا على اختلاف مكانتها وقدرتها التكنولوجية. هل تمكنت برامج الحماية والإجراءات الوقاية مهما كانت درجة تطورها من الصمود اما الاختراق الالكتروني الذي يهدد انظمة المعلومات الموجودة على مستوى القطاعات الهامة الاقتصادية والأمنية والدفاعية في إطار اتفاقية بودابست؟ للتوسع أكثر في الموضوع تم توظيف كل من المنهج التاريخي والوصفي والتحليلي.

تم التوصل في الأخير الى جملة من النتائج مفادها انه رغم محاولة اتفاقية بودابست ونجاحها النسبي في الإحاطة بالجريمة الالكترونية الا أن الطابع المتجدد والمتطور وعنصر المفاجئة الذي يميز هذه الجريمة ناهيك عن مهارة مرتكبها يجعل الخطر قائما دائما

الكلمات المفتاحية: الجريمة الالكترونية، دول أوروبا، اتفاقية بودابست.

Abstract:

Cybercrime is one of the most dangerous crimes that security systems face, especially countries in general, with different status and technological capabilities. Were the protection programs and preventive measures, regardless of their degree of development, able to withstand the electronic intrusion that threatens the existing information systems at the level of important economic, security and defense sectors withing the framework of the Budapest agreement? To expand further on the subject, both the historical, descriptive and analytical method were employed. Finally, a number of results were reached according to which despite the Budapest agreement's attempt and its relative success in covering cybercrime, the renewed and advanced nature and the element of surprise that characterizes this crime, not to mention the skill of its perpetrators makes the danger always present.

Keywords: cybercrime, European countries, Budapest convention.

مقدمة:

شهد الانسان خلال مسيرة حياته العديد من التطورات التي ساهمت بشكل كبير في تغيير مسار حياته من بينها ثورة تكنولوجيا المعلومات التي أدت لتغيير المجتمعات الحالية بشكل جوهري وتغيير شكل الحياة المستقبلية أيضا نتيجة اجتياح هده التكنولوجيا طافة جوانب الأنشطة البشرية.

أدت تكنولوجيا المعلومات لإحداث تطور إيجابي على مستوى عديد المجالات مثل الاتصالات السلكية واللاسلكية، تبادل كميات هائلة من البيانات بما في دلك الصوت والنص والموسيقى والصورة المتحركة، البريد الالكتروني، المواقع الالكترونية أدت كلها لإحداث طفرة تكنولوجية اقتصادية واجتماعية.

إلا أنها سامت أيضا في ظهور أنواع جديدة من الاجرام المتعلق بتكنولوجيا الاعلام تحت مسمى الجرائم الالكترونية.

إشكالية البحث:

من خلال ما سبق التطرق اليه يمكننا طرح التساؤل التالي فيما تكمن الجريمة الالكترونية؟ وهل تمكنت اتفاقية بودابست من الالمام بكافة جوانب هده الجريمة والنجاح في مكافحتها؟

منهج البحث:

لإشكالية البحث وطبيعة الموضوع دور رئيسي ومهم في اختيار المنهج المناسب الدي يجب اتباعه والاستناد عليه في تناول موضوع البحث، بناءا عليه تم اعتماد المنهج الوصفي من خلال وصف ظاهرة الجريمة الالكترونية بتعريفها وتحديد عناصرها بالإضافة التاريخي لدراسة مراحل تطور الجريمة الالكترونية والظروف التي مرت بها والمنهج التحليلي من خلال تحليل بنود اتفاقية بودابست وام ما ورد فيها من التزامات وإجراءات خدمة لموضوع البحث.

أهمية البحث وأهدافه:

- ✓ تصنف الجريمة الالكترونية ضمن أخطر الجرائم التي عرفتها البشرية في الآونة الأخيرة كونها تهدد امن المعلومات اما بحذفها او اختراقها او نشرها او بالتلاعب بها.
- ✓ تسليط الضوء على المجهودات المبذولة من طرف الدول الأوروبية في إطار اتفاقية بودابست سواء من حيث التحقيقات وتبادل الخبرات والمساعدات القضائية وتسليم المجرمين لتحقيق هدف موحد هو درأ خطر الجريمة الالكترونية عنها.
- ✓ تقييم محتوى الاتفاقية بتسليط الضوء على الجوانب التي تم التطرق اليها من حيث ايجابياتها وسلبياتها مرفقة بتوصيات بشأنها

أولا-الإطار المفاهيمي للجريمة الالكترونية:

مرت الجريمة الالكترونية بعدة مراحل ساهمت في انتشارها والتصعيد من مدى خطورتها ذلك نظرا لاقترانها بعناصر أساسية لا يمكن للإنسان الاستغناء عنها في حياته اليومية هي جهاز الكمبيوتر والشبكة العنكبوتية ونظم المعلومات مما يعني استمرارية حدوث هذا النوع من الجرائم بصفة متفاوتة من دولة لأخرى حسب أنظمة الحماية المعتمدة من قبلها.

1.تطور الجريمة الالكترونية:

ظهرت جرائم الانترنت نهاية الثمانينات ارتبطت بعمليات اقتحام نظام الكمبيوتر عن بعد وانشطة نشر وزرع الفيروسات الالكترونية التي تتولى عملية تدمير الملفات او البرامج ذلك عن طريق شخص الهاكر الذي يتولى عملية اقتحام النظم وتجاوز امن المعلومات باستخدام تفوقهم التقني بهدف الاستيلاء على الأموال او التجسس او الاستيلاء على البيانات السرية الاقتصادية والسياسية والعسكرية (مراد:2019، ص. 43).

بينما شهدت فترة التسعينات تناميا هائلا في مجال الجرائم الالكترونية وتغيير نطاق ومفهومها نتيجة الثروة التي أحدثتها شبكة الانترنت التي سهلت عملية دخول الأنظمة واقتحام شبكة المعلومات اذ شهدت حالات تعطيل النظم التقنية ومنعها من العمل المعتاد خاصة ما تعلق بمواقع الانترنت التسويقية الهامة التي يؤدي انقطاعها من الخدمة ساعات لخسائر مادية بالملايين بالإضافة لجرائم نشر الفيروسات عبر المواقع الالكترونية مما يسهل عملية الانتقال والولوج لصفحات المستخدمين واستخدامها بشكل غير مشروع (مراد:2019، ص. 44).

2.تعريف الجريمة الالكترونية:

تعد الجريمة الالكترونية جريمة مستحدثة ذات صنف جديد من الجرائم يعتمد مرتكبها على نظم معلوماتية وتكنولوجيا الاتصالات مما يعد انتقال من الصورة القديمة التقليدية للجريمة الى صورة حديثة يصعب التحكم فيها والتعامل معها.

لم يتفق جمهور الباحثين والدارسين وحتى التشريعات الوطنية على مفهوم موحد يتضمن العناصر الأساسية المكونة للجريمة المعلوماتية الامر الذي يفسره تعدد التسميات التي أطلقت عليها نجد تسمية الجريمة الالكترونية، جرائم الانترنت، جرائم الكمبيوتر، جرائم المعالجة الالية للبيانات والمعطيات (شوقي:2019، ص. 18).

عرفها البعض بأنها كل سلوك غير مشروع يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات، او هي كل نشاط غير مشروع موجه لنسخ او حذف او الوصول الى المعلومات المخزنة داخل الحاسوب او التي تحول عن طريقه. حيث تم التركيز على موضوع الجريمة المعلوماتية (الشكري:2008، ص.113).

بينما ذهب البعض الاخر لتقديم تعريف قائم على وسيلة ارتكابها يتمثل في انها نشاط اجرامي تستخدم فيه تقنية الحاسب بطريقة مباشرة او غير مباشرة بهدف تنفيذ العمل الاجرامي المقصود (وهيب:2014، ص. 338).

لا يوجد تعريف محدد المعالم للدلالة على الظاهرة الحديثة حيث ركز كل تعريف على عناصر معينة تختلف عن بقية التعاريف الأخرى.

تعد الجريمة المعلوماتية كل فعل او امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلومات يهدف للاعتداء على الأموال او الأشياء المعنوية. هي كل فعل اجرامي متعمد أيا كانت صلته بالمعلوماتية ينشأ عنه خسارة تلحق بالمجني عليه او كسب يحققه الفاعل (مومني:2008، ص. 20).

كما عرفت بأنها الجرائم التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا، هي جريمة متطلب لاقترافها ان تتوفر لدى فاعلها معرفة بتقنية الحاسوب (عياد:2008، ص. 40).

3.خصائص الجريمة الالكترونية

للجريمة الالكترونية خصائص وسمات عديدة تميزها عن غيرها من الجرائم تتمثل أهمها في:

- **الجرائم الالكترونية من الجرائم العابرة للحدود:** وسعت شبكات المعلومات عملية الاتصال وتبادل المعلومات بين الدول والأنظمة نتيجة القدرة التي يتمتع بها الحاسوب الالي نتج عنه إمكانية ارتكاب الجريمة الالكترونية في أماكن متعددة من العالم في وقت واحد يمكن أيضا عدم تواجد الجاني والمجني عليه في مكان واحد (إبراهيم:2008، ص. 82).

مسرح الجريمة الالكترونية لم يعد محليا او على نطاق وطني بل أصبح عالمي النطاق اذ ان الفاعل لا يتواجد بشكل مادي ملموس في مسرح الجريمة اذ يستطيع القيام بجريمته الدخول الى ذاكرة الحاسوب الالي الموجود في بلد اخر لإحداث ضرر لأكثر من شخص او هيئة (نعيم:2012، ص.32).

- **صعوبة اكتشاف وإثبات الجرائم الالكترونية:** الجريمة المعلوماتية لا تترك اثارا ملموسة ولا تترك شهود يمكن الاستدلال بأقوالهم ولا ادلة مادية يمكن فحصها كونها تحدث في بيئة افتراضية يتم فيها نقل المعلومات وتناولها بواسطة نبضات الكترونية غير مرئية او بإدخال رموز وأرقام وتوظيف تقنيات معقدة يصعب اكتشافها وإثباتها من قبل خبير او محقق تقليدي كونها تتطلب المام خاص بتقنيات الكمبيوتر ونظم المعلومات المتطورة (نعيم:2012، ص.34).

يصعب العثور على دليل مادي للجريمة بسبب استخدام الجاني وسائل فنية وتقنية معقدة في كثير من الأحيان هذا السلوك المادي لا يستغرق الا ثواني معدودة يتم خلالها محو أي دليل او التلاعب به (فريد:1994، ص. 82).

- **يتطلب ارتكابها وسائل خاصة:** يستلزم للقيام بتنفيذ الجريمة الالكترونية توفر جهاز الحاسوب الآلي وشبكة الانترنت والمعرفة التقنية للقائم بالجريمة ووجود خبرة وتحكم في تكنولوجيا المعلومات لا تستطيع الأجهزة الأمنية التعامل معه بشكل آني (نعيم:2012، ص.15).

- **أقل جهد وعنف في التنفيذ:** لا تتطلب الجرائم المعلوماتية عنف لتنفيذها كونها تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية التي تتطلب نوعا من المجهود العضلي الذي قد يكون في صورة ممارسة العنف والايذاء كما هو الحال في جرائم القتل والاختطاف والخلع والكسر والسرقة (شوقي:2019، ص.29-30).

تمتاز كونها من الجرائم الهادئة او الناعمة لا تحتاج في ممارسته الى العنف كل ما تحتاجه عامل الخبرة والذكاء والقدرة على التعامل مع جهاز الحاسوب بمستوى تقني عالي لارتكاب الأفعال غير المشروعة باستخدام ارقام وبيانات ليس لها أثر خارجي مادي (الرشيدي:2016، ص. 34).

- **دوافع مختلفة تدفع لارتكابها:** تختلف دوافع ارتكاب الجريمة الالكترونية عن غيرها من الجرائم الأخرى التقليدية من حيث الدوافع فقد تكون لمخالفة النظام العام والخروج عن القوانين وقد تكون أسباب مادية لكسب مبالغ مادية طائلة او للثأر والانتقام والاهانة ونشر معلومات سرية او الابتزاز (الصغير:2001، ص.88).

ثانيا-دور اتفاقية بودابست في الإحاطة ومكافحة الجريمة الالكترونية:

تصنف اتفاقية بودابست من الاتفاقيات القليلة المهمة التي ابرمت على نطاق إقليمي ساهمت في معالجة الجريمة الالكترونية من جوانب محددة بحصر أنواع لها وفرض التزامات محددة على الدول الأطراف فيها بغية تفعيل هذه المجهودات وتحقيق نتائج إيجابية مشجعة لإبرام مزيد من الاتفاقيات والتنويع في سبل مكافحتها.

1.الإطار التعريفي بالاتفاقية:

تعد معاهدة بودابست أولى المعاهدات المتعلقة بمكافحة جرائم الانترنت تم ابرامها في العاصمة المجرية بودابست بتاريخ 23 نوفمبر 2001 من طرف لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة بتاريخ 8 نوفمبر 2001بمناسبة المؤتمر الدولي حول الجريمة الالكترونية حيث اعتبر التوقيع عليها خطوة أولى من نوعها غاية في الأهمية في مجال محاربة هذا النوع من الجرائم (الجهيني:2004، ص.96).

وقعت على المعاهدة 26 دولة أوروبية بالإضافة إلى كندا واليابان وجنوب إفريقيا والولايات المتحدة الامريكية توفر المعاهدة أسس الأمن العام للمعلومات تضمنت 48 مادة موزعة على أربعة فصول (هلالي:2001، ص. 30).

دخلت الاتفاقية حيز التنفيذ شهر جويلية سنة 2004 تعد وثيقة دولية ملزمة بالنسبة للدول الأطراف فيها(الحسناوي:2009، ص. 147) تضمنت الاتفاقية فصول أربعة تناولت اجمالا بعض التعريفات الفنية لبعض المصطلحات ذات العلاقة وتحديد الجرائم التي تعتبر من اكثرها شيوعا على مستوى العالم محددة الطرق والإجراءات الواجب اتخاذها على المستوى الوطني للدول الأعضاء(الزهاني:2020، ص.430) خاصة الجنائية منها الرامية للحفاظ على المعلومات المخزنة بالإضافة لمسائل التعاون الدولي وتسليم المجرمين والتعاون في اطار جمع البيانات والتحقيقات والمسائل المتعلقة بالانضمام والانسحاب وتعديل المعاهدة والتشاور بين الاعضاء(فضل:2007، ص.430).

تهدف الاتفاقية بشكل أساسي الى مواءمة عناصر القانون الموضوعي الجنائي المحلي والاحكام المتصلة بالجرائم في مجال الجريمة الالكترونية، منح صلاحيات للقانون الاجرائي الجنائي الوطني الداخلي للتحقيق في هذا النوع من الجرائم ومتابعتها قضائيا علاوة على الجرائم الأخرى التي ترتكب عن طريق نظام الكمبيوتر أو التي تكون الأدلة المتصلة بها في شكل الكتروني إضافة الى انشاء نظام سريع وفعال للتعاون الدولي (خبراء:2001، ص. 04).

2. أنواع الجرائم الالكترونية التي حددتها اتفاقية بودابست:

قسمت الى أربع أنواع أساسية حسب اتفاقية بودابست تتمثل في:

- **الجرائم التي تمس خصوصية وسلامة وتوافر بيانات ونظم الكمبيوتر** تتمثل في النفاذ الكامل او الجزئي الى نظام الكمبيوتر بشكل متعمد بنية الحصول على بيانات الكمبيوتر او بأي نية غير صادقة أخرى، الاعتراض باستخدام وسائل

فنية للإرسال غير العمومي لبيانات الكمبيوتر الى أو من أو داخل نظام كمبيوتر بما في ذلك الانبعاثات الكهرومغناطيسية الصادرة عن نظام كمبيوتر يحمل هذا البيانات، الاتلاف العمدي لبيانات حاسوبية او حذفها او افسادها او تعديلها او تدميرها، التسبب العمدي في إعاقة خطيرة تتعلق باشتغال نظام الكمبيوتر عن طريق ادخال بيانات حاسوبية او ارسالها او اتلافها او حذفها او افسادها او تغييرها او تدميرها، حيازة كلمة سر خاصة بكمبيوتر او رمز الولوج او بيانات مماثلة يمكن بواسطتها النفاذ بشكل كامل او جزئي الى نظام الكمبيوتر بغرض ارتكاب جرائم إلكترونية (المواد من 2 الى 6اتفاقية بودابست:2001).

- **الجرائم ذات الصلة بالكمبيوتر** هي عبارة عن أفعال مجرمة إذا ما ارتكبت بصفة عمدية بنية الاحتيال وبغير حق مثل التزوير المرتبط بالكمبيوتر ذلك عن طريق ادخال أو تغيير أو حذف أو اتلاف بيانات كمبيوتر بشكل يجعل بيانات غير اصلية تبدو أصلية قصد استخدامها لأغراض معينة، الاحتيال المرتبط بالكمبيوتر الذي يرتكب عمدا يتسبب في الحاق خسارة بملكية شخص اخر عن طريق ادخال او تغيير او حذف أو اتلاف بيانات الكمبيوتر أو أي تدخل في وظيفة الكمبيوتر للحصول بدون وجه حق على منفعة اقتصادية ذاتية أو لفائدة شخص اخر(المواد من 7 الى 8 اتفاقية بودابست:2001).

- **الجرائم ذات الصلة بالمحتوى** تتمثل في الجرائم ذات الصلة بمواد إباحية عن الأطفال (يقصد بمواد اباحية عن الأطفال المواد الإباحية التي تعرض بشكل مرئي تحتوي على قاصر او شخص يبدو قاصر أو صور واقعية تظهر قاصر يمارس سلوك جنسي واضح) التي ترتكب عمدا وبغير حق كإنتاج مواد إباحية عن الأطفال أو حيازتها وعرضها وتوزيعها وإتاحتها أو نقلها عبر نظم الكمبيوتر أو وضعها داخله او الحصول عليها لصالح الشخص أو لفائدة الغير (المادة 9 من اتفاقية بودابست:2001)

- **الجرائم المتعلقة بانتهاكات حقوق النشر والتأليف والحقوق ذات الصلة** في حال ارتكابها عمدا على نطاق تجاري بواسطة نظام الكمبيوتر.

يتم أيضا فرض العقوبات وتحمل المسؤولية من خلال وضع التدابير التشريعية للدول الأعضاء تجرم أفعال ترتكب عمدا تشمل المساعدة أو التحريض على ارتكاب الجرائم السابقة أو محاولة ارتكابها، مساءلة الأشخاص الاعتباريين عن الجرائم التي ترتكب لمصلحتها من قبل أي شخص طبيعي سواء قام بذلك بمفرده أو باعتباره عضو في هيئة تابعة للشخص الاعتباري يعمل تحت سلطته هذا حسب ماورد في نص المادتين 11 و12 من اتفاقية بودابست.

اما بالنسبة لفرض العقوبات يتم ذلك في حال ارتكاب الجرائم السابقة الذكر تكون فعالة متناسبة مع نوع الفعل ورادعة بما في ذلك العقوبات السالبة للحرية سواء للأشخاص الطبيعيين او الاعتباريين بفرض عقوبات وتدابير جنائية أو غير جنائية منها العقوبات المالية.

من ناحية أخرى تسعى كل دولة طرف الى ضمان خضوع وضع وتنفيذ وتطبيق السلطات للإجراءات والضمانات والشروط المنصوص عليها في قانونها الوطني الذي ينبغي أن يوفر الحماية الملائمة لحقوق الانسان والحريات اذ تشمل هذه الشروط والضمانات حسب الاقتضاء بالنظر لطبيعة الإجراءات والسلطات المعنية الاشراف القضائي او بواسطة أي هيئة مستقلة أخرى، الأسس المبررة للتطبيق، حدود نطاق تلك الإجراءات ومدتها ذلك بقدر ما يتفق مع المصلحة العامة خاصة الإدارة السليمة للعدالة حيث يتم إقرار الولاية القضائية للدولة الطرف على الجرائم السابقة الذكر

عندما ترتكب داخل اقليمها او على متن سفينة ترفع علمها او على متن طائرة مسجلة بموجب قوانينها او من قبل احد مواطنيها او في حال تواجد الجاني داخل اقاليمها حسب ما ورد في المواد 12و 13 و 20 من الاتفاقية.

3.التدابير والإجراءات التي تتخذها الدول الأطراف في إطار مكافحة الجريمة الالكترونية:

- **التعجيل في حفظ بيانات الكمبيوتر المخزنة** اذ تعتمد كل دولة طرف ما يلزم من تدابير تشريعية وغيرها لتمكين سلطاتها المختصة من الامر او الحصول على الحفظ المعجل لبيانات كمبيوتر محددة بما في ذلك بيانات الحركة المخزنة بواسطة نظام الكمبيوتر خاصة في حال وجود أسس للاعتقاد ان تلك البيانات معرضة بشكل خاص للضياع او التعديل، عبر توجيه امر الى شخص من اجل حفظ بيانات كمبيوتر محددة ومخزنة بحوزته او تحت سيطرته وإلزامه بحفظ هذه البيانات والإبقاء على سلامتها لأطول مدة زمنية ضرورية على الا تتجاوز 90 يوما من أجل تمكين السلطات المختصة من التماس الكشف عنها مع الزامه بالحفاظ على سرية هذه الإجراءات طيلة الفترة الزمنية المحددة طبق القوانين الوطنية هذا حسب المادة 16.

- **التعجيل في حفظ بيانات الكمبيوتر والكشف الجزئي عن بيانات الحركة** اذ تعتمد الدول الأطراف ما يلزم من تدابير تشريعية وغيرها بهدف ضمان توفر إمكانية التعجيل في حفظ بيانات الحركة وتحديد مزود الخدمة والمجال الذي تم من خلاله نقل الاتصال.

- **الأمر بإبراز البيانات** ذلك بإصدار أمر الى أي شخص داخل أراضيها بتقديم بيانات كمبيوتر محددة بحوزته او تحت سيطرته مخزنة على نظام الكمبيوتر او دعامة أخرى للتخزين، أو إلى مزود خدمة يعرض خدماته بتقديم معلومات عن المشترك(هي معلومات مدرجة في شكل بيانات الكمبيوتر أو في أي شكل آخر يحفظها مزود الخدمة تتعلق بالمشتركين في الخدمات يمكن بموجبها تحديد هوية المشترك وعنوانه البريدي أو الجغرافي ورقم هاتفه والبيانات الخاصة بالفواتير والدفع المتاحة واي معلومات أخرى عن موقع تركيب أجهزة ومعدات الاتصال المتاحة) ذات الصلة بالخدمات الموجودة بحوزته او تحت سيطرته حسب ما ورد في المادة 18.**البحث عن بيانات الكمبيوتر المخزنة ومصادرتها** عن طريق قيام السلطات المختصة من البحث عن أو النفاذ الى أي نظام كمبيوتر او أي جزء منه وبيانات الكمبيوتر الخاصة فيه، أي دعامة تخزين بيانات الكمبيوتر مخزنة داخلها على أراضي الدولة الطرف مع قيام سلطاتها المختصة بمصادرة أو تامين بيانات الكمبيوتر التي تم النفاذ الها من خلال إجراء نسخة من هذه البيانات الحاسوبية والاحتفاظ بها والحفاظ على سلامة البيانات المخزنة ذات الصلة.

زيادة على ذلك يتم اعتماد تدابير تشريعية وغيرها تمكن من امر أي شخص لديه معرفة بتشغيل نظام الكمبيوتر او التدابير المطبقة لحماية البيانات الحاسوبية الموجودة عليه بتقديم في حدود المعقول المعلومات اللازمة حسب نص المادة 19 من الاتفاقية.

- **جمع بيانات الكمبيوتر في الوقت الحقيقي** ذلك من خلال قيام سلطاتها المختصة بجمع أو تسجيل من خلال تطبيق وسائل فنية على أراضيها أو اجبار مزود الخدمة في نطاق قدرته الفنية على التعاون مع السلطات المختصة ودعمها في جمع او تسجيل بيانات الحركة في الوقت الحقيقي ذات صلة باتصالات محددة على أراضيها تم نقلها بواسطة نظام

كمبيوتر مع الالتزام بسرية تنفيذ هذه الإجراءات من قبل مزود الخدمة ذلك في نطاق محاربة الجرائم الجسيمة التي يحددها القانون الوطني هذا طبقا لمحتوى المادة 20 من الاتفاقية.

- **تسليم المجرمين المرتكي للجريمة الالكترونية** نجم عن سهولة هروب المتهمين من الخضوع الى العقوبة في الجرائم السيبرانية وتعذر وصعوبة ملاحقتهم الى لجوء الدول الى الية تسليم وتتبع المجرمين حيثما كانوا لكيلا يفلتوا من العقاب وبالتالي يتمكن من محاربة الجريمة وحماية المجتمعات ممن يخلون بأمنها واستقرارها على المستوى الدولي والداخلي حتى لا يظل هؤلاء بمأمن من العقاب (الصغير:2001، ص. 88).

إذن نظام تسليم المجرمين هو اجراء تعاون دولي تقوم بمقتضاه دولة تسمى الدولة المطلوب اليها بتسليم شخص يوجد في اقليمها الى دولة ثانية تسمى بالدولة الطالبة او جهة قضائية دولية، بهدف ملاحقته عن جريمة اتهم بارتكابها او لأجل تنفيذ حكم جنائي صدر ضده (سليمان:2015، ص.33).

حسب ما ورد في المادة 24 من الاتفاقية يتم تسليم المجرمين بين الدول الأطراف حيث يعاقب بعقوبة سالبة للحرية مدة سنة على الأقل او بعقوبة اشد كما يمكن تطبيق عقوبة اقل من سنة في حال وجود تشريع موحد أو ذي صلة بالمعاملة بالمثل او بموجب معاهدة تسليم المجرمين فيكون التسليم شرط للمحاكمة حيث يخضع للشروط التي ينص عليها قانون الدولة الطرف المطلوب منها التسليم او معاهدات تسليم المجرمين الواجبة التطبيق بما في ذلك الأسباب التي تستند اليها الدولة الطرف المطالبة بالتسليم لرفض التسليم.

- **المساعدة المتبادلة بين الدول الأطراف في إطار تحقيق العدالة** يتم ذلك بين الدول الأطراف في الاتفاقية على أوسع نطاق ممكن لغرض التحقيق أو المتابعة المتعلقة بالجرائم الجنائية ذات الصلة بنظم وبيانات الكمبيوتر او بجمع ادلة جريمة جنائية في شكل الكتروني، ناهيك عن اعتمادها ما يلزم من تدابير تشريعية وغيرها، المطالبة بالمساعدة المتبادلة بمنح وثائق عن طريق وسائل الاتصال العاجلة بما في ذلك الفاكس أو البريد الالكتروني بقدر ما توفره من امن وصحة البيانات واستخدام التشفير عند الضرورة حيث تقبل الدولة الطرف المطلوب منها تقديم المساعدة وتستجيب للطلب بوسائل الاتصال العاجلة .

هذا ويجوز لدولة طرف في حدود قانونها الوطني دون طلب مسبق ارسال معلومات يتم الحصول علها في إطار التحقيقات التي تنجزها الى طرف اخر إذا ما رأت أن الإفصاح عنها قد يساعد في تحقيقات أو متابعات بشأن جرائم جنائية حسب مضمون المادة 25 من اتفاقية بودابست.

خاتمة:

من خلال ما سبق دراسته والتطرق اليه من عناصر أساسية تمكنا من استخلاص جملة من النتائج أهمها

- ✓ تحديد الاتفاقية لأنواع الجرائم الالكترونية تحديدا دقيقا.
- ✓ وضع تدابير للتعاون بين الدول الأعضاء وحثهم على مكافحة هذا النوع من الجرائم الذي يشكل خطورة كبيرة على الدول الأوروبية خاصة كونها رائدة في المجال الالكتروني.

- ✓ الإرادة الفعالة والحقيقية للدول الأوروبية العضوة لمواجهة الجرائم الالكترونية من خلال وضع اليات تعاون عديدة تكمن في التعاون القضائي والإجرائي والمعلوماتي وتسليم المجرمين والمساعدة المتبادلة.
- ✓ وجود صعوبات تشكل عائق حقيقي في وجه الدول الأطراف تتمثل في اختلاف الأنظمة القانونية والإجرائية فيما بينها من حيث التحري أو التحقيق أو الاختصاص القضائي او تسليم المجرمين.

في هذا الصدد ارتأينا اقتراح التوصيات التالية:

- ✓ إيجاد سبل واليات قانونية وقضائية تواكب السرعة والطبيعة المتغيرة والمتجددة للجريمة الالكترونية وخصوصيتها.
- ✓ اعتماد نظم إجرائية وتشريعات وطنية محددة لسد الثغرات والقضاء على الاختلافات وحالات تنازع الاختصاص القضائي.

قائمة المراجع:

1) إبراهيم، خالد ممدوح (2008): أمن الجريمة الالكترونية، الدار الجامعية. الإسكندرية.
2) اتفاقية الجريمة الالكترونية بودابست 20011.
3) الجهيني، منير محمد، الجهيني، ممدوح محمد (2004): جرائم الانترنت والحاسب الالي ووسائل مكافحتها، دار الفكر العربي. الاسكندرية.
4) الحسناوي، علي جبار (2009): جرائم الحاسوب والانترنت، دار اليازوري. الأردن.
5) الرشيدي، طه السيد احمد (2016): الطبيعة الخاصة لجرائم تقنية المعلومات وأثرها على إجراءات التحقيق في النظام الجزائي المصري والسعودي، دار الكتب والدراسات. الإسكندرية.
6) الزهاني، شيخة حسن (2020): التعاون الدولي في مواجهة الهجوم السيبراني، مجلة جامعة الشارقة للعلوم القانونية، العدد 01. مجلد17.
7) سليمان، عبد المنعم (2015): الجوانب الإشكالية في النظام القانوني لتسليم المجرمين دار المطبوعات الجامعية.
8) الشكري، عادل يوسف عبد النبي (2008): الجريمة المعلوماتية وأزمة الشرعية الجزائية، مجلة الكوفة. مركز دراسات الكوفة. العراق. العدد 07.
9) شوقي، يعيش (2019): الجريمة المعلوماتية: دراسة تأصيلية مقارنة، ط1. مطبعة الرمال. الوادي. الجزائر.
10) الصغير، جمال عبد الباقي (2001): الجوانب الإجرائية للجرائم المتعلقة بالأنترنت، دار النهضة العربية. مصر.
11) عياد، سامي علي حامد (2008): الجريمة المعلوماتية، دار الفكر الجامعي. الاسكندرية.
12) فريد، هشام محمد (1994): الجوانب الإجرائية للجرائم المعلوماتية، ط1، مكتبة الآلات الحديثة.

13) فضل، سليمان احمد (2007): المواجهة التشريعية والأمنية للجرائم الناشئة عن استخدام شبكة المعلومات الدولية، دار النهضة العربية.

14) مجموعة خبراء (2001): التقرير التفسيري لاتفاقية الجريمة الالكترونية، مجلس أوروبا. بودابست.

15) مراد، عبد الفتاح (د.ت): دور الكمبيوتر في مجال ارتكاب الجرائم الالكترونية، دار الكتب والوثائق المصرية. مصر.

16) مومني، نهلا عبد القادر (2008): الجرائم المعلوماتية، ط1، دار الثقافة للنشر والتوزيع.

17) نعيم، سعيد (2012): اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري، مذكرة مقدمة لنيل شهادة الماجستير. جامعة الحاج لخضر. باتنة. الجزائر.

18) هلالي، عبد الله احمد (2001): الجوانب الموضوعية والاجرائية للجرائم المعلوماتية على ضوء اتفاقية بودابست 2001، دار النهضة العربية.

19) وهيب، مشتاق طالب (2014): مفهوم الجريمة المعلوماتية ودور الحاسب في ارتكابها، مجلة العلوم القانونية والسياسية. جامعة ديالي.العراق.العدد01. المجلد 02.

الجرائم الالكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in the Islamic jurisprudence and the positive law

د. كرم سلام عبد الرؤوف سلام/ جامعة عين شمس/مصر

رئيس قسمي الاقتصاد والتجارة الإلكترونية، كلية العلوم الإدارية، جامعة باشن العالمية بأمريكا

Dr. Karam Salam Abdel Raouf Salam/ Ain Shams University/ Egypt

Head of the Departments of Economics and E-Commerce, College of Administrative Sciences, Passion International University, USA

ملخص الدراسة:

يهدف البحث إلى: التعرف على ومناقشة وتحليل موضوع الجرائم الالكترونية فى الفقه الإسلامي والقانون الوضعى، وذلك من خلال استعراض الجريمة الالكترونية ماهيتها ومعرفة أسبابها وأركانها، والجريمة الالكترونية وسبل مكافحتها، وموقف الشريعة الإسلامية من الجريمة المعلوماتية، وإثبات الجريمة من الناحية الشرعية والقانونية، ومواكبة النصوص العقابية في القانون للنصوص في الشريعة الاسلامية. والتعرف على تجارب الدول الأخرى في ردع أصحاب هاته الجريم ومدى مواكبة نصوص القوانين العقابية في الدول العربية للدول المتقدمة في هذا الجانب. بإستخدم المنهج الوصفى التحليلى. وقد **توصلت الدراسة إلى**: أن الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت.

الكلمات المفتاحية: الجرائم الالكترونية، الفقه الإسلامي، القانون الوضعى

Abstract:

The research aims to: identify, discuss and analyze the subject of cybercrime in Islamic jurisprudence and positive law, by reviewing the nature of cybercrime, knowing its causes and pillars, cybercrime and ways to combat it, the position of Islamic law on information crime, proving the crime in terms of legitimacy and legality, and keeping pace with the texts. Punitive law for texts in Islamic law. And getting to know the experiences of other countries in deterring the perpetrators of this crime and the extent to which the texts of the penal laws in the Arab countries keep pace with the developed countries in this aspect. Using the descriptive analytical method. **The study concluded**: that cybercrime is an act that causes serious harm to individuals, groups, and institutions with the aim of blackmailing the victim and tarnishing its reputation to achieve material gains or serve political goals by using modern means and systems of communication such as the Internet.

Keywords: cybercrime, Islamic jurisprudence, positive law.

1.مقدمة:

لقد شهد القرن الماضى ثورة في مجال التكنولوجيا والاتصالات، مما أدى لظهور أجيال جديدة من وسائل الاتصال عن بعد، والتى أعادت صياغة شكل العالم فأصبح العالم قرية صغيرة لا تعرف الحدود، وبالطبع تم الاستفادة من هذه التكنولوجيا في مختلف القطاعات الحياتية في الدولة، وعلى جميع المستويات خاصة بعد تطور نظم المعلومات وربطها بالأقمار الصناعية، وبالطبع تعقدت الجريمة وتنوعت أساليب ارتكابها مستفيدة من هذا التطور التقنى المذهل

فظهر ما يعرف بجرائم التقنية أو الجرائم المعلوماتية التى أخذت أبعادا جديدة بداية من ثمانينات القرن الماضي، حيث كانت بدايات انتشار الحاسب الآلي وتطبيقاته بشكل عام، لحقه انتشار شبكة الإنترنت في بداية التسعينيات من ذات القرن، هذه الأخيرة التى برزت كأسرع وأقوى وسائل اتصال حديثة في العالم اليوم. وتعد الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت"، ويحدث ذلك من خلال القذف والتشهير الالكتروني، السرقة الإلكترونية، النصب والاحتيال الإلكتروني، والتزوير الالكتروني، والإرهاب الالكتروني.

وتعد الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت. ويمكن وبحسب البيئات والوسائل المختلفة المستخدمة، تحدث الجريمة الإلكترونية دون تواجد الجاني في مكان الحدث، وتستند الطريقة المستخدمة إلى تكنولوجيا الاتصالات والمعلومات الحديثة. إن عدد الجرائم الالكترونية في انتشار واسع نظرا للتطور الحاصل في التكنولوجيا سواء في وسائل التواصل الاجتماعي أو عبر الدول مما أضر باقتصادها ومختلف تعاملاتها، كما أن الأساليب الإجرامية اختلفت وتنوعت من قبل متمرسين في هذا الجانب.

وبما أن الشريعة رادعة في جانب العقوبات فاشتملت على عقوبات توقف كل مجرم يتجاوز حدود الله تعالى ويسعى في الأرض فسادا والله لا يحب المفسدين. وجاء القانون أيضا معاقبا كل من تسول له نفسه الاعتداء على حقوق الناس بالسلب أو النهب أو الظلم. كما ان هناك عدة انواع للجرائم الالكترونية وتتمثل في سرقة الهوية حيث يقوم فيها المجرم بإغراء الضحية واستخراج المعلومات منه بشكل غير مباشر ، واستهداف المعلومات الخاصة من أجل الربح واستغلالها لتحقيق مكاسب مادية وأيضا تهديد الأفراد حيث يقوم المجرم، من خلال القرصنة وسرقة المعلومات ، بالوصول إلى المعلومات الشخصية الخاصة بالضحية ، ثم ابتزازهم لكسب المال وتحريضهم على ارتكاب أعمال غير قانونية قد يتعرضون فيها للظلم ، وكذلك من الأنواع التشهير حيث يستخدم المجرم المعلومات المسروقة ويضيف اليها معلومات كاذبة ثم يرسلها عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني لكثير من الناس بهدف تشويه سمعة الضحية وتدميرها نفسياً.وغيرها من الأنواع المتعددة في هذا المجال . إن خطر الجريمة الالكترونية خطر عظيم تجاوز كل الحدود والأعراف وأصبح يهدد الأشخاص والدول، لذا وجب الحد من هذا التفاقم المتزايد بمعاقبة المجرمين عقابا صارما دون تردد أو تأخير. الجريمة الالكترونية يصعب اثباتها جراء التعقيدات التي في ثناياها لان من السهولة اخفاء دليل اثباتها لذلك يجد المحققون صعوبة جمة في إثبات أدلة الجريمة.

2.إشكالية البحث:

إن الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت.

ويمكن وبحسب البيئات والوسائل المختلفة المستخدمة، تحدث الجريمة الإلكترونية دون تواجد الجاني في مكان الحدث، وتستند الطريقة المستخدمة إلى تكنولوجيا الاتصالات والمعلومات الحديثة. إن عدد الجرائم الالكترونية في

انتشار واسع نظرا للتطور الحاصل في التكنولوجيا سواء في وسائل التواصل الاجتماعي آو عبر الدول مما أضر باقتصادها ومختلف تعاملاتها، كما أن الأساليب الإجرامية اختلفت وتنوعت من قبل متمرسين في هذا الجانب.

وبما أن الشريعة رادعة في جانب العقوبات فاشتملت على عقوبات توقف كل مجرم يتجاوز حدود الله تعالى ويسعى في الأرض فسادا والله لا يحب المفسدين. وجاء القانون أيضا معاقبا كل من تسول له نفسه الاعتداء على حقوق الناس بالسلب أو النهب أو الظلم. كما ان هناك عدة انواع للجرائم الالكترونية وتتمثل في سرقة الهوية حيث يقوم فيها المجرم بإغراء الضحية واستخراج المعلومات منه بشكل غير مباشر، واستهداف المعلومات الخاصة من أجل الربح واستغلالها لتحقيق مكاسب مادية وأيضا تهديد الأفراد حيث يقوم المجرم، من خلال القرصنة وسرقة المعلومات، بالوصول إلى المعلومات الشخصية الخاصة بالضحية، ثم ابتزازهم لكسب المال وتحريضهم على ارتكاب أعمال غير قانونية قد يتعرضون فيها للظلم

وكذلك من الأنواع التشهير حيث يستخدم المجرم المعلومات المسروقة ويضيف اليها معلومات كاذبة ثم يرسلها عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني لكثير من الناس بهدف تشويه سمعة الضحية وتدميرها نفسياً.وغيرها من الأنواع المتعددة في هذا المجال.

إن خطر الجريمة الالكترونية خطر عظيم تجاوز كل الحدود والأعراف وأصبح يهدد الأشخاص والدول، لذا وجب الحد من هذا التفاقم المتزايد بمعاقبة المجرمين عقابا صارما دون تردد أو تأخير. الجريمة الالكترونية يصعب اثباتها جراء التعقيدات التي في ثناياها لان من السهولة اخفاء دليل اثباتها لذلك يجد المحققون صعوبة جمة في اثبات ادلة الجريمة.

مما سبق: تتضح إشكالية البحث في محاولة الإجابة على التساؤلات التالية:

- ✓ ماهو موقف الشريعة الاسلامية والقانون الوضعي من الجريمة المعلوماتية؟
- ✓ ماهي الطرق المنوطة بإثبات هاته الجرائم؟
- ✓ كيفية تعامل الجهات المختصة مع هذا النوع من الجرائم؟
- ✓ ماهي الحلول المكنة للحد من هاته الجرائم وسبل مكافحتها؟
- ✓ ما مدى مواكبة المشرع العربي للقوانين المعاصرة في مجال المعلوماتية؟

3.أهداف البحث:

يهدف البحث إلى التحقق من والتعرف على النقاط التالية:

- ✓ الجريمة الالكترونية ماهيتها ومعرفة أسبابها وأركانها
- ✓ الجريمة الالكترونية وسبل مكافحتها
- ✓ موقف الشريعة الإسلامية من الجريمة المعلوماتية.
- ✓ إثبات الجريمة من الناحية الشرعية والقانونية.
- ✓ مواكبة النصوص العقابية في القانون للنصوص في الشريعة الاسلامية.
- ✓ التعرف على تجارب الدول الأخرى في ردع أصحاب هاته الجريم.

- ✓ مدى مواكبة نصوص القوانين العقابية في الدول العربية للدول المتقدمة في هذا الجانب.

4.أهمية البحث:

ترجع أهمية البحث من أهمية موضوع الجريمة الإلكترونية، حيث ان الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت. ويمكن وبحسب البيئات والوسائل المختلفة المستخدمة، تحدث الجريمة الإلكترونية دون تواجد الجاني في مكان الحدث، وتستند الطريقة المستخدمة إلى تكنولوجيا الاتصالات والمعلومات الحديثة. إن عدد الجرائم الالكترونية في انتشار واسع نظرا للتطور الحاصل في التكنولوجيا سواء في وسائل التواصل الاجتماعي أو عبر الدول مما أضر باقتصادها ومختلف تعاملاتها، كما أن الأساليب الإجرامية اختلفت وتنوعت من قبل متمرسين في هذا الجانب.

5.فرضية البحث:

تنطوى فرضية البحث الرئيسية عن فرضية مؤدها " ان الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت"، ويحدث ذلك من خلال القذف والتشهير الالكتروني، السرقة الإلكترونية، النصب والاحتيال الالكتروني، ولتزوير الالكتروني، والإرهاب الالكتروني، ومحاولة الاجابة على تساؤلات البحث.

6.تساؤلات البحث:

يهدف البحث إلى محاولة الإجابة على التساؤلات التالية:

- ✓ ما هو الإطار المفاهيمى للجريمة الالكترونية؟
- ✓ ما هى الجرائم المتصلة بالجرائم الالكتروني؟
- ✓ ما هو دور مختلف المؤسسات في مكافحة الجريمة الالكترونية؟
- ✓ ماهو موقف الشريعة الاسلامية والقانون الوضعي من الجريمة المعلوماتية؟
- ✓ ماهي الطرق المنوطة بإثبات هاته الجرائم؟
- ✓ كيفية تعامل الجهات المختصة مع هذا النوع من الجرائم؟
- ✓ ماهي الحلول المكنة للحد من هاته الجرائم وسبل مكافحتها؟
- ✓ ما مدى مواكبة المشرع العربي للقوانين المعاصرة في مجال المعلوماتية؟

7.منهجية البحث:

تقوم منهجية البحث على أتباع المنهج الوصفى التحليلى للتعرف على واستعراض وتحليل الإطار المفاهيمى للجريمة الالكترونية، والجرائم المتصلة بالجرائم الالكترونية، ودور مختلف المؤسسات في مكافحة الجريمة الالكترونية، موقف الشريعة الاسلامية والقانون الوضعي من الجريمة المعلوماتية، الطرق المنوطة بإثبات هاته الجرائم، وكيفية تعامل الجهات المختصة مع هذا النوع من الجرائم، الحلول الممكنة للحد من هاته الجرائم وسبل مكافحتها، ومدى

مواكبة المشرع العربي للقوانين المعاصرة في مجال المعلوماتية، ودور مختلف المؤسسات (المحاكم والقضاء، والنيابة العامة ،والمخابر الجنائية) فى مواجهة الجرائم الالكترونية.

8.نطاق البحث:

يتم تقسيم نطاق وحدود البحث للأتى:

- ✓ النطاق المكانى: دراسة تطبيقية على مستوى العالم
- ✓ النطاق الزمانى: خلال عام ٢٠١٠ وحتى ٢٠٢٢
- ✓ النطاق القطاعى: قطاع تكنولوجيا المعلومات والاتصالات
- ✓ النطاق التطبيقى: الفقة الإسلامى والقانون الوضعى

9.الدراسات السابقة:

هناك عدد من الدراسات التى تناولت ظاهرة الجرائم الالكترونية ومنها مايلي:

-**دراسة**: بعنوان: الجرائم الالكترونية: المفهوم والأسباب، تهدف الدراسة إلى: دراسة مفهوم الجرائم الالكترونية والأسباب التى تؤدى إليها، وقد توصلت الدراسة إلى: أن الجرائم الالكترونية ظاهرة إجتماعية متوافقة مع انتقال المجتمع للتحول الرقمى، وأن الجرائم الالكترونية هى جرائم عابرة الحدود والوطنية (ذياب: ٢٠١٨، ص.١-٤٩٥).

-**دراسة** : بعنوان : الجريمة الإلكترونية وسبل مواجهتها فى الشريعة الإسلامية والأنظمة الدولية: دراسة تحليلية تطبيقية ،تهدف الدراسة إلى: دراسة مفهوم الجرائم الالكترونية وسبل مواجهتها في الشريعة الإسلامية والأنظمة الدولية، وقد توصلت الدراسة إلى: أن الشريعة الإسلامية تمتاز بأنها شريعة عالمية تواكب كل زمان، والحاسب الآلي والانترنت لهم إيجابيات وسلبيات، ومرتكب الجرائم الالكترونية هو شخص يتميز بالذكاء والدهاء وهو ذو مهارات تقنية عالية وهو شخص إنسجاميا وإجتماعيا وقادر ماديا إلا أن باعثة لإرتكاب الجرائم الالكترونية هو رغبته فى قهر النظام والجريمة الالكترونية ذات بعد دولى وعابرة الحدود(ابراهيم :٢٠١٥، ص١-٢٥) .

-**دراسة**: بعنوان جرائم التزوير الالكترونية: دراسة مقارنة، تهدف الدراسة إلى: دراسة مفهوم جريمة التزوير الالكترونية وأركانها وأنواعها وعقوبة التزوير الالكترونية، وقد توصلت الدراسة إلى: أن جريمة التزوير الالكترونية حديثة النشأة وتختلفعن جريمة التزوير التقليدية من حيث الوسيلة المستخدمة فى إرتكابها حيث يشترط فى جريمة التزوير الالكترونية استخدام الحاسب الالي فى حين جريمة التزوير التقليدية لا تشترط استخدام وسيلة معينة، وقوبة جريمة التزوير الالكترونية السجن المؤقت (حفصي :٢٠١٥، ص.١-٢٥٤) .

10. خطة البحث:

يتم تقسيم البحث للنقاط التالية:

١-الإطار العام للجريمة الالكترونية

٢-الجرائم المتصلة بالجرائم الالكترونية

٣-مواجهة الجرائم الالكترونية وطرق إثباتها

٤-دور مختلف المؤسسات في مكافحة الجريمة الالكترونية

مقدمة:

:

أدى التطور المتلاحق للإنترنت وانتشار أجيال جديدة وأنواع مختلفة من أجهزة الحاسب الآلي إلى مضاعفة المخاطر والاعتداءات على الحريات الشخصية والملكية الخاصة، بل وعلى مصالح الدولة مما حذا ببعض الدول أن تقر اتفاقيات تقرر تجريم بعض الأفعال الحادثة عبر الوسائل الالكترونية أو بواسطتها، ومنها اتفاقية بودابست لعام 2001، والقانون العربي النموذجي الموحد لمكافحة سوء استخدام تكنولوجيا المعلومات والاتصالات ،والذي تم اقراره من قبل وزراء العدل العرب في اجتماعهم المشترك في 12-2003/5/22، غير أننا لم نر له أثرا فعليا علي أغلب التشريعات الجنائية في الدول العربية وبصفة خاصة مصر، فلا يوجد بها حتى الآن تشريع جنائي خاص بالجريمة الالكترونية يقدم الحلول الناجعة لكافة المشكلات القانونية الناجمة عنها على الرغم من وجود بعض النصوص القانونية التى تحتويها قوانين تنظم موضوعات مختلفة تناولت بعض صور التجريم الالكتروني ،منها قانون الأحوال المدنية المصري رقم 143 لسنة 1994 ، قانون حماية الملكية الفكرية رقم 82 لسنة 2002، قانون تنظيم الاتصالات 10 لسنة 2003، وقانون التوقيع الالكترونى 15 لسنة 2004، وقانون الطفل المعدل في 2008، إلا أن هذه القوانين لم تغط كافة صور التجريم الالكتروني ، وهو ماكان له أثره السيء علي المجتمع بسبب عدم توفير الحماية القانونية لأفراده خصوصا في ظل وجود مبدأ دستوري يحكم التجرم في مصر وهو مبدأ الشرعية الجنائية والذي ورد النص عليه في المادة 95 من الدستور المصري الحالي الصادر في عام 2014 ،والتى جرى نصها على أن " العقوبة شخصية، ولا جريمة ولا عقوبة إلا بناء على قانون ،ولا توقع عقوبة إلا بحكم قضائي ولا عقاب إلا على الأفعال اللاحقة لتاريخ نفاذ القانون"، فمع وجود ذلك النص الدستوري وغياب النص التشريعى العقابي يصبح القاضي الجنائي في حيرة من أمره خصوصا عندما يعرض عليه فعل يشكل جريمة من الجرائم الالكترونية التي لا يجد لها نصا صريحا يجرمها في قانون العقوبات، فكيف السبيل الى الحكم الشافي ؟ هل يحكم بالبراءة إعمالا لمبدأ شرعية التجريم؟ أم يحاول إنزال حكم القانون في الجرائم التقليدية على تلك الجريمة أخذا بالتفسير القضائي الواسع للنصوص القانونية؟ ذاك ما نصبو في هذا البحث الإجابة عنه من خلال تحديد هذه المعضلة القانونية الواقعة (ذياب: ٢٠١٨، ص.١-٤٩٥).

تعد الجريمة الالكترونية فعل يتسبب في ضرر جسيم للأفراد والجماعات والمؤسسات بهدف ابتزاز الضحية وتشويه سمعتها لتحقيق مكاسب مادية أو لخدمة أهداف سياسية باستخدام وسائل وأنظمة اتصال حديثة مثل الإنترنت. ويمكن وبحسب البيئات والوسائل المختلفة المستخدمة، تحدث الجريمة الإلكترونية دون تواجد الجاني في مكان الحدث، وتستند الطريقة المستخدمة إلى تكنولوجيا الاتصالات والمعلومات الحديثة. إن عدد الجرائم الالكترونية في انتشار واسع نظرا للتطور الحاصل في التكنولوجيا سواء في وسائل التواصل الاجتماعي آو عبر الدول مما أضر باقتصادها ومختلف تعاملاتها، كما أن الأساليب الإجرامية اختلفت وتنوعت من قبل متمرسين في هذا الجانب. وبما أن الشريعة رادعة في جانب العقوبات فاشتملت على عقوبات توقف كل مجرم يتجاوز حدود الله تعالى ويسعى في الأرض فسادا والله لا يحب المفسدين. وجاء القانون أيضا معاقبا كل من تسول له نفسه الاعتداء على حقوق الناس بالسلب أو النهب أو الظلم. كما ان هناك عدة انواع للجرائم الالكترونية وتتمثل في سرقة الهوية حيث يقوم فيها المجرم بإغراء الضحية واستخراج المعلومات منه بشكل غير مباشر، واستهداف المعلومات الخاصة من أجل الربح واستغلالها لتحقيق

مكاسب مادية وأيضا تهديد الأفراد حيث يقوم المجرم، من خلال القرصنة وسرقة المعلومات، بالوصول إلى المعلومات الشخصية الخاصة بالضحية ، ثم ابتزازهم لكسب المال وتحريضهم على ارتكاب أعمال غير قانونية قد يتعرضون فيها للظلم ،وكذلك من الأنواع التشهير حيث يستخدم المجرم المعلومات المسروقة ويضيف اليها معلومات كاذبة ثم يرسلها عبر وسائل التواصل الاجتماعي أو البريد الإلكتروني لكثير من الناس بهدف تشويه سمعة الضحية وتدميرها نفسياً.وغيرها من الأنواع المتعددة في هذا المجال . إن خطر الجريمة الالكترونية خطر عظيم تجاوز كل الحدود والأعراف وأصبح يهدد الأشخاص والدول، لذا وجب الحد من هذا التفاقم المتزايد بمعاقبة المجرمين عقابا صارما دون تردد أو تأخير. الجريمة الالكترونية يصعب اثباتها جراء التعقيدات التي في ثناياها لان من السهولة اخفاء دليل اثباتها لذل قصك يجد المحققون صعوبة جمة في اثبات أدلة الجريمة.

1.الإطار العام للجريمة الالكترونية:

التعامل الالكتروني أصبح من ضروريات الحياة اليومية لكل شخص، وهو ضرورة للعمل والدراسة وحتى الترفيه والاتصالات الشخصية مع الأصدقاء والمجموعات. والتعاملات الالكترونية ذللت الكثير من النشاطات الخاصة والأعمال الرسمية نظرا لتوفيرها للمعلومات والبيانات والبحوث وغيرها، ومن هذا استفاد ويستفيد الجميع. ومن دون شك، فإن الثورة التقنية أثرت على حياتنا ومفاهيمنا واستفدنا منها كثيرا. ولكن، هناك من يفكر في الاستفادة الإجرامية ويعمل على تسخير التعامل والتطور الالكتروني في ارتكاب الجرائم والأفعال المخالفة للقانون والمعاملات والأعراف والآداب. من هنا نشأت الجريمة الالكترونية، وهي تعتبر من الجرائم الحديثة التي ظهرت بعد انتشار الثورة التقنية التي نعيشها ونستمتع بمخرجاتها. والجريمة، عموما، قديمة وظهرت مع بداية البشرية بين أول أخوين. وكما يقول علماء النفس، فإن النزعة الإجرامية موجودة في البشر بدرجات متفاوتة، ولكن هناك من يسيطر عليها وهناك من لا يستطيع ويرتكب الجريمة سواء العادية التقليدية أو تلك الالكترونية الحديثة.

1.1. تعريف الجريمة الالكترونية:

تعرف الجريمة إصلاحا بجرائم الإنترنت (Computer crime)جرائم التقنية العالية (Hi-tech crime)الجريمة السيبرانية (Cyber crime ، ولقد أدت الحداثة التي تتميز بها الجريمة الإلكترونية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة الإلكترونية من بينها: فحسب اللجنة الأوروبية فان مصطلح الجريمة الإلكترونية يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات، ونشر مواد إلكترونية ذات محتوى مخل بالأخلاق أو دعوى لفتن طائفية. وحسب وزارة العدل في الولايات المتحدة الأمريكية التي عرفت الجريمة عبر الإنترنت بأنها "اي جريمة لفاعلها معرفة فنية بتقنية الحاسبات تمكنه من ارتكابها"، وحسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الإنترنت "هي كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات ونقلها".

تعرف الجريمة الإلكترونية على أنها "الاعتداء غير القانونى الذي يرتكب بواسطة المعلومات الحاسوبية بغرض تحقيق الربح.... "كما عرفت بأنها" كل فعل إجرامي متعمد أيا كانت صلته بالمعلومات ينشأ عنه خسارة تلحق بالمجنى عليه أو كسب يحققه الفاعل وعرفت أيضا بأنها" كل فعل غير مشروع يكون العلم بتكنولوجيا الحاسبات الآلية بقدر كبير لازما لارتكابها من ناحية، ولملاحقته وتحقيقه من ناحية أخرى"، بينما عرفها فريق آخر بأنها" كل جريمة تتم في

محيط أجهزة الكمبيوتر" أو هي" كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات أو بنقلها (ذياب: ٢٠١٨، ص.١-٤٩٥).

، كما تعرف أيضا بأنها" كل نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة أو غير مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامى المقصود". كما تعرف الجريمة الإلكترونية على أنها " هي نشاط إجرامي يستهدف أو يستخدم جهاز كمبيوتر أو شبكة كمبيوتر أو جهازاً متصلاً بالشبكة، ترتكب معظم الجرائم الإلكترونية من قبل مجرمي الإنترنت أو المتسللين الذين يريدون جني الأموال، ويتم تنفيذ الجرائم الإلكترونية من قبل الأفراد أو المنظمات (ذياب: ٢٠١٨، ص.١-٤٩٥)." وقال القاضي باركر «هي كل فعل إجرامي متعمد إذا كانت صلته بالمعلوماتية تنشأ عن خسارة تلحق بالمجني عليه أو كسب يحققه الفاعل..». والمنظمة الأوربية للتعاون والتنمية الاقتصادية (أو إي سي دي) عرفت الجريمة الالكترونية والمعلوماتية «بأنها كل سلوك غير مشروع أو مناف للأخلاق وغير مسموح به ويرتبط بالمعالجة الآلية للبيانات أو بنقلها». والقاضي ناديمان عرفها «بأنها الجريمة التي تلعب فيها بيانات الكمبيوتر والبرامج المعلوماتية دورا رئيسيا، وأنها تستهدف سرية المعلومات وسلامتها ووجودها والأجهزة ومحتوياتها بغرض تخريبها». وهناك من يقول إن الجريمة الالكترونية هي عبارة عن مجموعة أنشطة غير مشروعة تستهدف المعلومات بطريقة تمكن الاطلاع عليها أو تزييفها أو حذفها وذلك بوسائط تقنية المعلومات.

بعض مجرمي الإنترنت منظمون ويستخدمون تقنيات متقدمة ولديهم مهارات فنية عالية، البعض الآخر قراصنة مبتدئين، ونادرًا ما تهدف الجرائم الإلكترونية إلى إتلاف أجهزة الكمبيوتر لأسباب أخرى غير الربح، يمكن أن تكون هذه سياسية أو شخصية. وكما هو معلوم، فإن الجريمة الالكترونية وبالرغم من حداثتها إلا أن آثارها مضرة ومدمرة لأبعد الحدود لأنها قد تهز العالم بمجرد كبس أو ضرب زر الجهاز. وقانونا، نقول إن هناك صعوبات جمة في تعريف الجريمة الالكترونية وهذا قد يؤدي إلى إفلات المجرم بجريمته نظرا لعدم وضوح تعريف هذه الجريمة الحديثة. ومن المبادئ العدلية والدستورية الأساسية «لا عقوبة بلا جريمة»، و» لا جريمة ولا عقوبة إلا بنص»، ولذا لا بد من الحرص على تعريف الجريمة الالكترونية وتحديد أركانها وأنماطها وأشكالها بوضوح حتى تتم معاقبة مرتكبها.. (ولكم في القصاص حياة). ومن ضمن محاولات تعريف الجريمة الالكترونية، هي كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات.

ومعلوم أنها تستخدم الكمبيوتر والآلات الذكية كأداة استخدام للجريمة. والجريمة الالكترونية، تدور حولنا في خفاء تام ودون أن نشعر بها لأنها في الأثير (جريمة سبرانية) الطلق، وخطورة هذه الجريمة الخفية أنها تغطي كل المجالات المالية والحسابات المصرفية والعمليات البنكية، وتتدخل في أخص الخصوصيات وتنتهك الأعراض والذمم، وحتى تضر بأمن الدول وتتجسس عليها.. وهكذا، فهي تحوم في كل الاتجاهات وفي كل الأوقات، وتعمل بسوء نية لتحقيق مصالح دنيئة لا يقبلها القانون ولا الأعراف، ولا ينجو منها أحد مهما كان صغيرا أو كبيرا. ومن هنا تأتي الخطورة. ولكن، كما يتضح لنا، فإن تعريف الجريمة الالكترونية، ما زال في مرحلة الآراء والدراسات والأفكار من القانونيين والتشريعيين وفنيي تقنية المعلومات، ونتطلع إلى نهج وأسلوب واضحين يضعان هذه الجريمة الخطيرة في إطارها ومعناها الصحيح،

حتى تتم محاربتها ومواجهتها فنيا وتشريعيا، وهذا ضروري لحماية الثورة التقنية وتمكينها من التطور لخدمة البشرية وأخذها إلى مجالات تقنية أرحب وأشمل.

2.1.نشأة وتطور الجرائم الالكترونية:

مرت الجرائم الالكترونية بعدد من المراحل وهي كما يلي(ذياب: ٢٠١٨، ص.١-٤٩٥):

المرحلة الأولى: تمتد من شيوع استخدام الحاسب الآلي في الستينات إلى غاية 1970، اقتضت معالجة على المقالات تمثلت في التلاعب بالبيانات المخزنة وتدميرها.

المرحلة الثانية: في الثمانينات حيث طفح على السطوح مفهوم جديد لجرائم الكمبيوتر والإنترنت تمثلت في اقتحام الأنظمة ونشر الفيروسات.

المرحلة الثالثة: في التسعينات حيث شهدت هذه المرحلة تناميا هائلا في حقل الجرائم الإلكترونية، نظرا لانتشار الإنترنت في هذه الفترة مما سهل من عمليات دخول الأنظمة واقتحام شبكة المعلومات مثلا: تعطيل نظام تقني، نشر الفيروسات...الخ (ابراهيم :٢٠١٥، ص.٣٦٠-٤٠٣).

3.1.أركان الجرائم الالكترونية:

تقوم الجرائم الالكترونية على أركان ومنها (ذياب: ٢٠١٨، ص.١-٤٩٥):

الركن المادي: ترتبط طبيعة الركن المادي في الجرائم الإلكترونية بالمشكلات المُثارة. ويقصد بذلك سوء استخدام الأنظمة الإلكترونية بطريقة غير مشروعة، أو اقتحام آثار مادية ملموسة تساهم في التدمير للمعلومات، أو السرقة لبطاقات الائتمان أو التزوير والتلاعب في البيانات المرتبطة بالحواسب الآلية. وإن السلوك الإجرامي يعتبر عنصر أساسي في الركن المادي في الجرائم التقليدية، كمشاهدة الجاني ورؤيته رؤية العين في قيامه بالقتل أو السرقة أو التزوير، أمّا في الجرائم الإلكترونية فيكون من الصعب أن يتم ارتكاب أو امساك الجاني مادياً؛ وذلك لأنَّها عبارة عن جرائم ترتكب من خلال المعلومات والبيانات المتوافرة عبر أنظمة الحواسب الآلية (ذياب: ٢٠١٨، ص.١-٤٩٥).

الركن المعنوي: ويقصد به الحالة النفسية والمزاجية لمرتكبي الجرائم الإلكترونية، مع أهمية التركيز على العلاقات التي تكون مرتبطة ما بين ماديات الجريمة وشخصية الجاني.

الركن الشرعي: ويقصد به الصفات غير المشروعة للفعل، حيث يكون هنالك قاعدة تجريم وعقوبات مفروضة على الجرائم الإلكترونية المرتبطة بأنظمة المعلومات.

ويكون السلوك الإجرامي مرتبط أيضاً بالمعلومات المخّزنة، أو التي يتم إدخالها إلى الحاسب الآلي. وقد يتمثل السلوك الإجرامي أيضاً في تدمير النظام المعلوماتي أو التزوير؛ وذلك من خلال التسلل إلى أرصدة الحسابات المتوافرة في البنوك.

4.1.أسباب ودوافع ارتكاب الجرائم الالكترونية:

هناك عدد من الأسباب والدوافع لارتكاب الجرائم الالكترونية ومنها ما يلى (ابراهيم :٢٠١٥، ص.٣٦٠-٤٠٣):

دوافع مادية ويتمثل في: تحقيق الكسب المادي: تعد الرغبة في تحقيق الثراء من العوامل الرئيسية لارتكاب الجريمة عبر الإنترنت. نظرا للربح الكبير، وغالبا ما يكون الدافع لارتكاب هذه الجريمة هو وقوع الجاني في مشاكل مادية مثال على ذلك تحويل حساب مالي إلى حسابه.

دوافع شخصية وتتمثل في: الرغبة في التعلم يكرس مرتكبو هذه الجريمة وقته في تعلم كيفية اختراق المواقع الممنوعة والتقنيات الامنية للأنظمة الحاسوبية.

دوافع ذهنية أو نمطية: غالبا ما يكون الدافع لدى مرتكب الجرائم عبر الإنترنت هو الرغبة في اثبات الذات وتحقيق الانتصار على تقنية الانظمة المعلوماتية دون ان يكون لهم نوايا اثمة.

دافع الانتقام تعد من أخطر الدوافع التي يمكن ان تنفع شخص يملك معلومات كبيرة عن المؤسسة أو شركة يعمل بها تجعله يقدم على ارتكاب جريمته.

دافع التسلية هي جريمة ترتكب من اجل التسلية لايقصد من ورائها احداث جرائم.

دافع سياسي يتم غالبا في المواقع السياسية المعادية للحكومة، ويتمثل في تلفيق الاخبار والمعلومات ولو زورا أو حتى الاستناد إلى جزء بسيط جدا من الحقيقة ومن ثم نسخ الاخبار الملفقة حولها، تعد الدوافع السياسية من أبرز المحاولات الدولية لاختراق شبكات حكومية في مختلف دول العالم.

وجدير بالذكر أن الدافع لارتكاب جرائم الإنترنت يختلف عن دافع الجرائم التقليدية، فالبعض يرتكب الجريمة الالكترونية لولعه في الحصول على المعلومات الجديدة مثل القراصنة، أو للاستيلاء على المعلومات الموجودة على جهاز الكمبيوتر أو حذفها أو تدميرها أو الغائها نهائيا، وقد يكون الدافع الرغبة في قهر النظام الالكتروني بغرض تحقيق شهرة وإثبات التفوق العلمى لديه، وهي تكون بين الشباب، وقد تكون لاستهداف بعض الأشخاص والجهات.

5.1. أشكال الجرائم الالكترونية:

تتعدد أشكال الجرائم الالكترونية ومنها ما يلي:

- ✓ اقتحام شبكات الحاسب الالي وتخريبها (قرصنة البرامج).
- ✓ سرقة المعلومات أو الاطلاع عليها بدون ترخيص.
- ✓ انتهاك الاعراض وتشويه السمعة.
- ✓ اتلاف وتغيير ومحو البيانات والمعلومات.
- ✓ تسريب المعلومات والبيانات.
- ✓ جمع المعلومات والبيانات وغعادة استخدامها.
- ✓ نشر واستخدام برامج الحاسب الالي بما يشكل انتهاك لقوانين حقوق الملكية والاسرار التجارية.

6.1.تصنيف الجرائم الالكترونية:

تتعدد صور الجريمة الالكترونية " الجريمة المعلوماتية" إلا أنها تتفق جميعها في الوسيلة المستخدمة لارتكابها وهي الأجهزة التقنية الحديثة من حاسبات آلية وخلافها، وكلها تتم عبر شبكة الإنترنت، وقد عددت اتفاقية بودابست المتعلقة بالإجرام الكوني" الإجرام ر" والموقعة من الإتحاد الأوربي في 11/23 /2001، وصور الجرائم الالكترونية التي عددتها الاتفاقية هي الصور الممثلة للإجرام المعلوماتي الحادث الآن وتتمثل في الآتي (ذياب :٢٠١٤، ص.١-٢٥):

أولاً: الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية: وقد عددت الاتفاقية صور هذه الجرائم في الآتي:

الولوج غير القانونى: وهو يعني الدخول غير المشروع لنظام معلوماتي مملوك للغير " القرصنة" والتي قد تكون بهدف إتلاف أو تدمير النظام المعلوماتي للغير أو الحصول على معلومات وبيانات سرية مملوكة للغير أو التدخل بتغيير البيانات المخزنة في النظام المعلوماتي المملوك للغير وهو ما يطلق عليه الغش أو التزوير المعلوماتي.

الاعتراض غير القانونى: وهي جريمة انتهاك الحق في الخصوصية والتى تحدث عندما يتم اعتراض المراسلات الالكترونية والاتصالات الالكترونية الخاصة بالغير. وهذه الجريمة تتعلق بكافة أشكال النقل الالكتروني للبيانات سواء عن طريق التليفون أو الفاكس أو البريد الالكتروني أو غير ذلك من الوسائل التقنية الحديثة.

الاعتداء علي سلامة البيانات: وتتمثل في الاعتداء عمدا على البيانات والبرامج الخاصة بجهاز الحاسب الآلي المملوك للغير بهدف تعطيل الجهاز أو محو وطمس بيانات الحاسب الآلي.

الاعتداء على سلامة النظام: وهي تتمثل في الأفعال التي تحمل اعتداء على حسن تشغيل نظام الحاسب الآلي بشكل جسيم مما يؤدي لتوقف النظام عن العمل مثل الإعتداء من خلال استخدام الفيروسات.

إساءة استخدام أجهزة الحاسب: أي كل فعل مجرم قانونا يتم من خلال استخدام الحاسب الآلي.

ثانيا: الجرائم المعلوماتية المتصلة بالحاسب وتتمثل في الآتي (ذياب :٢٠١٤، ص.١-٢٥) :

-الاحتيال المعلوماتي أو التزوير و الغش المعلوماتيين : ويقصد به الخداع أو الغش المعلوماتي الذي يقوم علي التلاعب في نظم المعالجة الآلية للمعلومات بهدف الحصول دون وجه حق علي خدمات أو أموال أو أصول معينة، ويقوم الجاني في هذه الجريمة باستخدام التقنيات الحديثة بغية التلاعب في البيانات المصرفية ونتائج الميزانيات والمستحقات المالية، فيتم تحويل تلك الأموال في ثوانٍ معدودة من حساب إلى آخر، وتتمثل خطورة هذا الفعل الإجرامي في كونه يتم عبر الحدود الإقليمية لأكثر من دولة وفي ثوان معدودة، وهو ما يجعله بالغ الأثر السلبي على الاقتصاد القومى ؛ إذ من الممكن أن يؤدي ارتكاب مثل هذه الجريمة إلى إفلاس شركات أو بنوك كبرى في الدولة

-الجرائم المتصلة بمحتوى الحاسب الآلي: وهي تتعلق بجرائم إنتاج ونشر المواد الإباحية الخاصة بالأطفال وبيع الأطفال والإتجار فيهم والترويج لدعارة الأطفال.

-الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة: وهي تعد من الجرائم الالكترونية الأكثر شيوعا وانتشارا وتستهدف الأعمال الأدبية والتصويرية والموسيقية والسمعية البصرية، وذلك نظرا للسهولة التى يمكن من خلالها عمل نسخ غير مصرح بها عن طريق التكنولوجية الرقمية، مما يضر بالحقوق المالية للمالكين والمنتجين.

أما الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فلم تقم بعمل تصنيف مشابه للاتفاقية السابقة بل قامت بسرد للجرائم الالكترونية على سبيل المثال مثل جرائم استخدام وسائل المعلومات، وجرائم الاحتيال والإباحية، وجرائم الاستغلال الجنسي، وحرمة الاعتداء على الحياة الخاصة، وما يتعلق بالإرهاب والجريمة المنظمة.

وهناك من الفقه من صنف الجرائم الالكترونية تحت نوعين من الجرائم على حسب الأداة المستخدمة في ارتكابها: (ذياب :٢٠١٤، ص.١-٢٥):

النوع الأول: web crime computer وهو يتعلق بجرائم الشبكة العالمية التي تستخدم الحاسب وشبكاته كوسيلة مساعدة لارتكاب جريمة مثل استخدامه في النصب والاحتيال وغسل الأموال وتشويه السمعة والسب والقذف، وفي هذا النوع من الجرائم يكون الحاسب الآلي محتفظا بأدلة رقمية تساعد في كشف الفاعل.

النوع الثاني: crime computerوهو يتعلق بالجرائم التي يكون الحاسب فيها محلا للفعل الإجرامي ذاته كالأفعال الإجرامية الواقعة على مكونات الحاسب المادية، أو المكونات المعنوية soft wareأو قاعدة البيانات، date basesأو المعلومات التي قد تكون على الحاسب من خلال الحصول غير المشروع عليها ونشرها" انتهاك الملكية الفكرية"، أو من خلال تسجيل مواد اباحية عليه.

وهناك جانب أخر من الفقه قسم الجرائم الالكترونية إلى جرائم تقليدية: ترتكب عن طريق استخدام الحاسب الآلي وهي جرائم السرقة والنصب وخيانة الأمانة والاتلاف والتصنت إلى غير ذلك من الجرائم، وجرائم مستحدثة مثل جرائم التجسس والقرصنة، وبعضهم قسم الجرائم الالكترونية حسب المصلحة المحمية بالقانون إلى الجرائم الالكترونية التي تمثل الاعتداء على الأشخاص، والجرائم الالكترونية التي تمثل اعتداء على الأموال، والجرائم الالكترونية التي تمثل اعتداء على البيانات، والجرائم الالكترونية التي تمثل اعتداء على الآداب العامة وحقوق الملكية الفكرية، والجرائم الالكترونية ذات الصلة بالإجرام المنظم والجرائم السياسية .

ومما سبق تقديمه من تقسيمات يتضح أنه لكي يدخل الفعل في إطار الجرائم الالكترونية يجب أن يقوم جهاز الحاسب الآلي في الجريمة بدور على قدر من الأهمية، ويقصد بجهاز الحاسب الآلي في هذا المقام المكونات المنطقية للحاسب الآلي من معلومات وبرامج وكذلك جميع المكونات الأخرى التي تساعد في عملية المعالجة الآلية للمعلومات، ويكمن هذا الدور في كون النظام قد ساعد وسهل في ارتكاب الفعل على نحو كبير، ويختلف دور الحاسب الآلي في الجريمة الالكترونية من جريمة لأخرى

7.1. **أنواع الجرائم الالكترونية:**

عشرات الطرق التي يمكن من خلالها تفسير الجريمة الإلكترونية، وتحتاج إلى معرفة ماهيتها من أجل حماية نفسك، تحتاج إلى معرفة الطرق المختلفة التي يمكن من خلالها اختراق جهاز الكمبيوتر الخاص بك وانتهاك خصوصيتك. في هذا الجزء، نناقش أنواع الجرائم الإلكترونية الشائعة التي يستخدمها مجرمو الإنترنت (ابراهيم:٢٠١٥، ص٣٦٠-٤٠٣)

-القرصنة: القرصنة هي عمل يرتكبه متطفل عن طريق الوصول إلى نظام الكمبيوتر الخاص بك دون إذنك، المتسللون عادة يكونون مبرمجين كمبيوتر لديهم فهم متقدم لأجهزة الكمبيوتر وعادة ما يسيئون استخدام هذه المعرفة لأسباب خادعة. بعض الناس يفعلون ذلك لمجرد التباهي بخبراتهم، بينما يريد الآخرون فقط التسبب في التدمير، وقد يتسبب الجشع والميول المتلصصة في بعض الأحيان في قيام أحد المتطفلين باختراق أنظمة لسرقة المعلومات المصرفية الشخصية والبيانات المالية للشركة وما إلى ذلك.

- انتشار الفيروس: الفيروسات هي برامج كمبيوتر ترتبط أو تصيب نظاماً أو ملفات، وتميل إلى الانتشار إلى أجهزة كمبيوتر أخرى على الشبكة، إنها تعطل تشغيل الكمبيوتر وتؤثر على البيانات المخزنة -إما عن طريق تعديلها أو بحذفها تماماً.

عادة ما يُنظر إلى الفيروسات على أنها رمز غريب مرتبط ببرنامج مضيف، ولكن هذا ليس هو الحال دائماً، في بعض الأحيان يتم التلاعب بالبيئة بحيث يؤدي استدعاء برنامج شرعي غير مصاب إلى استدعاء البرنامج الفيروسي، ويمكن أيضاً تنفيذ البرنامج الفيروسي قبل تشغيل أي برنامج آخر.

عادة ما تنتشر فيروسات الكمبيوتر عبر الوسائط القابلة للإزالة أو عبر الإنترنت، قرص فلاش أو قرص مضغوط أو شريط مغناطيسي أو أي جهاز تخزين آخر كان موجوداً في جهاز كمبيوتر مصاب يصيب جميع أجهزة الكمبيوتر المستقبلية التي يتم استخدامه فيها. ويمكن لجهاز الكمبيوتر الخاص بك أيضاً التقاط فيروسات من مرفقات البريد الإلكتروني أو مواقع الويب الضارة أو البرامج المصابة، وتنتشر هذه على كل جهاز كمبيوتر آخر على شبكتك، وتتسبب جميع فيروسات الكمبيوتر في أضرار اقتصادية مباشرة أو غير مباشرة.

- **الشفرات**: الشفرات أو المعروفة باسم «القنابل الإلكترونية»، هي جزء خبيث من التعليمات البرمجية يتم إدخاله عمداً في البرنامج لتنفيذ مهمة ضارة عند تشغيلها بواسطة حدث معين، إنه ليس فيروساً رغم أنه عادة ما يتصرف بطريقة مماثلة.

يتم إدخاله خلسة في البرنامج حيث يظل في وضع السكون حتى يتم استيفاء الشروط المحددة، وغالباً ما تحتوي البرامج الضارة مثل الفيروسات على قنابل منطقية يتم تشغيلها في حمولة معينة أو في وقت محدد مسبقاً.

عادة ما يتم استخدام القنابل المنطقية من قبل موظفين ساخطين يعملون في قطاع تكنولوجيا المعلومات، وذلك لحذف قواعد بيانات أصحاب العمل، أو تسخير الشبكة لفترة أو حتى القيام بالتداول من الداخل، ويمكن أن تكون المشغلات المرتبطة بتنفيذ القنابل المنطقية عبارة عن تاريخ ووقت محددين، أو إدخال مفقود من قاعدة بيانات أو عدم وضع أمر في الوقت المعتاد، ما يعني أن الشخص لم يعد يعمل هناك.

-**اقتحام الويب**: في محاولة من المخترق أن يتحكم في موقع الويب بطريقة احتيالية، حتى يتحكم في تغيير محتوى الموقع الأصلي أو إحداث أي تغيير فيه أو مسح بيانات من عليه، تم الإبلاغ عن حالات طلب فيها المهاجم فدية، وحتى نشر مواد فاحشة على الموقع.

- المطاردة السيبرانية: تعد المطاردة عبر الإنترنت شكلاً جديداً من أشكال جرائم الإنترنت في مجتمعنا عندما يتم ملاحقة شخص ما أو ملاحقته عبر الإنترنت، والمطارد الإلكتروني لا يتبع ضحيته جسدياً، يفعل ذلك افتراضياً من خلال متابعة نشاطه عبر الإنترنت، لجمع معلومات حول المطارد ومضايقته أو توجيه تهديدات باستخدام التخويف اللفظي.

إنه انتهاك لخصوصية المرء على الإنترنت، وتستخدم المطاردة عبر الإنترنت أو أي وسيلة إلكترونية أخرى وتختلف عن المطاردة غير المتصلة بالإنترنت، ولكنها عادة ما تكون مصحوبة بها، ومعظم ضحايا هذه الجريمة هم من النساء الذين يلاحقهم الرجال. وتتم المطاردة عبر الإنترنت بطريقتين أساسيتين:

المطاردة عبر الإنترنت: هنا يقوم المطارد بمضايقة الضحية عبر الإنترنت، البريد الإلكتروني غير المرغوب فيه هو الطريقة الأكثر شيوعاً لتهديد شخص ما، وقد يرسل المطارد محتوى فاحشاً وفيروسات عبر البريد الإلكتروني.

-**مطاردة الكمبيوتر**: يستخدم الملاحقون الأكثر تقدماً من الناحية التكنولوجية مهاراتهم في الكمبيوتر لمساعدتهم في الجريمة، يكتسبون سيطرة غير مصرح بها على كمبيوتر الضحية من خلال استغلال عمل الإنترنت ونظام التشغيل Windows.

- **التلاعب بالبيانات** :هو تغيير غير مصرح به للبيانات قبل أو أثناء الدخول إلى نظام الكمبيوتر، ثم تغييرها مرة أخرى بعد انتهاء المعالجة، باستخدام هذه التقنية، قد يقوم المهاجم بتعديل الإخراج المتوقع ويصعب تتبعه، بمعنى آخر يتم تغيير المعلومات الأصلية التي سيتم إدخالها، إما عن طريق شخص يكتب البيانات، أو فيروس مبرمج لتغيير البيانات، أو مبرمج قاعدة البيانات أو التطبيق، أو أي شخص آخر يشارك في عملية الإنشاء والتسجيل أو ترميز البيانات أو فحصها أو فحصها أو تحويلها أو نقلها. هذه واحدة من أبسط الطرق لارتكاب جريمة متعلقة بالكمبيوتر، لأنه حتى هواة الكمبيوتر يمكنهم فعل ذلك، على الرغم من أن هذه مهمة سهلة، يمكن أن يكون لها آثار ضارة (ابراهيم:٢٠١٥، ص٣٦٠-٤٠٣) .

-**سرقة الهوية** والاحتيال على بطاقات الائتمان: تحدث سرقة الهوية عندما يسرق شخص ما هويتك ويتظاهر بأنه أنت للوصول إلى موارد مثل بطاقات الائتمان والحسابات المصرفية والمزايا الأخرى باسمك.

قد يستخدم المحتال أيضاً هويتك لارتكاب جرائم أخرى، «الاحتيال على بطاقة الائتمان» مصطلح واسع النطاق للجرائم التي تنطوي على سرقة الهوية حيث يستخدم المجرم بطاقة الائتمان الخاصة بك لتمويل معاملاته، الاحتيال على بطاقة الائتمان هو سرقة الهوية في أبسط أشكالها.

- قرصنة البرامج بفضل الإنترنت يمكنك العثور على أي فيلم أو برنامج أو أغنية من أي مكان تقريباً مجاناً، تعتبر قرصنة الإنترنت جزءاً لا يتجزأ من حياتنا والتي نساهم فيها جميعاً عن قصد أو عن غير قصد.

بهذه الطريقة، يتم تخفيض أرباح مطوري هذه الموارد، ولا يتعلق الأمر فقط باستخدام الملكية الفكرية لشخص آخر بشكل غير قانوني ولكن أيضاً بنقلها لأصدقائك ما يقلل من الإيرادات التي يستحقونها.

قرصنة البرامج هي الاستخدام والتوزيع غير المصرح به لبرامج الكمبيوتر، يعمل مطورو البرمجيات بجد لتطوير هذه البرامج، وتحد القرصنة من قدرتهم على توليد عائدات كافية لاستدامة تطوير التطبيقات، ويؤثر هذا على الاقتصاد العالمي بأكمله حيث يتم تحويل الأموال من القطاعات الأخرى، ما يؤدي إلى تقليل الاستثمار في التسويق والبحث.

-الجرائم ضد الافراد: وتسمى بجرائم الإنترنت الشخصية تتمثل في سرقة الهوية ومنها البريد الإلكتروني، أو سرقة الاشتراك في موقع شبكة الإنترنت وانتحال شخصية أخرى بطريقة غير شرعية عبر الإنترنت بهدف الاستفادة من تلك الشخصية أو لإخفاء هوية المجرم لتسهيل عملية الإجرام.

-الجرائم ضد الملكية: تتمثل في نقل البرمجيات الضارة المضمنة في بعض البرامج التطبيقية والخدمية أو غيرها، بهدف تدمير الأجهزة أو البرامج المملوكة للشركات أو الأجهزة الحكومية أو البنوك أو حتى الممتلكات الشخصية.

-الجرائم ضد الحكومات: مهاجمة المواقع الرسمية وأنظمة الشبكات الحكومية والتي تستخدم تلك التطبيقات على المستوى المحلي والدولي كالهجمات الإرهابية على شبكة الإنترنت، وهي تتركز على تدمير البنى التحتية ومهاجمة شبكات الكمبيوتر وغالبا ما يكون هدفها سياسي.

وفيما يلي بعض الأمثلة المحددة لأنواع الجرائم الالكترونية المختلفة: (ابراهيم:٢٠١٥، ص٣٦٠-٤٠٣)

- ✓ الاحتيال عبر البريد الالكتروني والإنترنت.
- ✓ تزوير الهوية (حيث تتم سرقة المعلومات الشخصية واستخدامها).
- ✓ سرقة البيانات المالية أو بيانات الدفع بالبطاقة.
- ✓ سرقة بيانات الشركة وبيعها.
- ✓ الابتزاز الالكتروني (طلب المال لمنع هجوم مهدد).
- ✓ هجمات برامج الفدية (نوع من الابتزاز الالكتروني).
- ✓ السرقة المشفّرة (حيث يقوم المتسللون بتعدين العملات المشفّرة باستخدام موارد لا يملكونها).
- ✓ التجسس الالكتروني (حيث يتمكن المتسللون من الوصول إلى بيانات حكومة أو شركة ما).
- ✓ تندرج معظم الجرائم الالكترونية ضمن فئتَين رئيسيتَين، هما:
- ✓ النشاط الإجرامي الذي يستهدف أجهزة الكمبيوتر.
- ✓ النشاط الإجرامي الذي يستخدم أجهزة الكمبيوتر لارتكاب جرائم أخرى.

8.1 أهداف الجرائم الالكترونية:

تهدف الجرائم الالكترونية للأتى: (ذياب :٢٠١٤، ص.١-٢٥):

التمكين من الوصول إلى المعلومات بشكل غير قانوني كسرقة المعلومات أو حذفها والإطلاع عليها.

التمكن من الوصول بواسطة الشبكة العنكبوتية إلى الاجهزة الخادمة الموفرة للمعلومات وتعطيلها أو التلاعب بمعطياتها مثل اداة المسح ((ncوتدعى سكينة الجيش السويسري في مجموعة ادوات الأمن بحيث تقدم هذه الاداة خدمة مسح قوية للبروتوكول الافتراضي وتنفذ بالشكل netcatوأيضا البروتوكول النقل tcpولمسح هذا البرتوكول يجب إضافة المعامل2 netcat -uاداة المسح ((strobeتستخدم لمسح منفذ بروتوكول النقل المضمون tcp.

الحصول على المعلومات السرية للجهات المستخدمة للتكنولوجيا كالبنوك والمؤسسات والحكومات والأفراد والقيام بتهديدهم اما لتحقيق هدف مادي أو سياسي

الكسب المادي أو المعنوي أو السياسي غير المشروع مثل تزوير بطاقات الائتمان وسرقة الحسابات المصرفية (ابراهيم:٢٠١٥، ص.٣٦٠-٤٠٣).

9.1 أدوات الجرائم الالكترونية:

تتعدد أدوات الجرائم الالكترونية ومنها: (محمد :٢٠٠٥، ص.٣٠-٦٥):

- ✓ برامج نسخ المعلومات المخزنة في اجهزة الحاسب الالي.
- ✓ الإنترنت كوسيط لتنفيذ الجريمة.
- ✓ خطوط الاتصال الهاتفي التي تستخدم لربط الكمرات ووسائل التجسس.
- ✓ ادوات مسح الترميز الرقمي (البا ركو د)
- ✓ الطابعات.
- ✓ اجهزة الهاتف النقال والهواتف الرقمية الثابتة.

✓ برامج مدمرة: مثل برنامج حصان طروادة trojan horseبحيث يقوم بخداع المستخدم لتشغيله، حيث يظهر على شكل برنامج مفيد وامن ويؤدي تشغيله إلى تعطيل الحاسب المصاب وبرنامج الدودة الذي يشبه الفيروس ولكنه يصيب اجهزة الحاسب دون الحاجة إلى اي فعل وغالبا يحدث عندما ترسل بريد إلكتروني إلى كل الأسماء الموجودة في سجل الأسماء.

10.1. **طبيعة وخصائص الجرائم الالكترونية:**

تتصف الجرائم الالكترونية بعدد من الصفات والخصائص تميزها عن غيرها من الجرائم التقليدية هي: (ابراهيم:٢٠١٥، ص٣٦٠-٤٠٣)

✓ سهولة ارتكاب الجريمة بعيدا عن الرقابة الأمنية، فهي ترتكب عبر جهاز الكمبيوتر مما يسهل تنفيذها من قبل المجرم دون أن يراه أحد أو يكتشفه.

✓ صعوبة التحكم في تحديد حجم الضرر الناجم عنه قياسا بالجرائم الإلكترونية فالجرائم الالكترونية تتنوع بتنوع مرتكبيها وأهدافهم وبالتالي لايمكن تحديد حجم الأضرار الناجمة عنها.

✓ مرتكبها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا صعبا أعمارهم تتراوح غالبا ما بين 18 إلى 48 سنة).

✓ تنطوي على سلوكيات غير مألوفة عن المجتمع.

✓ اعتبارها أقل عنفا في التنفيذ فهي تنفذ بأقل جهد ممكن مقارنة بالجرائم التقليدية، لأن المجرم عند تنفيذه لمثل هذه الجرائم لا يبذل جهدا فهي تطبق على الأجهزة الإلكترونية وبعيدا عن أي رقابة مما يسهل القيام بها.

✓ جريمة عابرة للحدود لا تعترف بعنصر المكان والزمان فهي تتميز بالتباعد الجغرافي واختلاف التوقيتات بين الجاني والمجني عليه، فالسهولة في حركة المعلومات عبر أنظمة التقنية الحديثة جعل بالإمكان ارتكابها عن طريق حاسوب موجود في دولة معينة بينما يتحقق الفعل الإجرامي في دولة أخرى.

✓ سهولة إتلاف الأدلة من قبل الجناة، فالمعلومات المتداولة عبر الإنترنت على هيئة رموز مخزنة على وسائط تخزين ممغنطة وهي عبارة عن نبضات إلكترونية غير مرئية مما يجعل أمر طمس ومحو الدليل أمر سهل.

✓ ترتكب بواسطة شبكة الإنترنت: أي تستخدم شبكة الإنترنت كأداة لارتكاب الجريمة أو تسهيل ارتكابها؛ إذ تعد شبكة الإنترنت حلقة الوصل بين كافة الأهداف المحتملة لتلك الجرائم كالبنوك والشركات بكافة أنواعها والأشخاص وغيرها، والتي غالبا ما تكون الضحية.

✓ مرتكب الجريمة مجرم ذو خبرة في استخدام الحاسب الآلي والإنترنت.

✓ الجرائم الالكترونية لا تعرف الحدود المكانية ولا الحدود الزمنية لأنها ترتكب عبر شبكة الإنترنت لا تحدها حدود جغرافية كحدود دولة بعينها، فالعالم كله يمكن أن يكون مسرحا لارتكاب الجريمة، كما لا يحدها زمان معين رغم الاختلاف في المواقيت بين الدول.

✓ الجرائم الالكترونية تتسم بالخطورة البالغة: وذلك من عدة نواحٍ فمن ناحية: الخسائر الناجمة عنها كبيرة جدا قياسا بالجرائم التقليدية وبصفة خاصة جرائم الأموال، ومن ناحية ثانية: نجدها ترتكب من فئات إجرامية متعددة تجعل من الصعب معرفة الفاعل، ومن ناحية أخيرة: تنطوي على سلوكيات غير مألوفة.

✓ صعوبة التحري والتحقيق في هذه الجرائم ومن ثم محاكمة مرتكبها: فهناك صعوبة في ملاحقة مرتكب هذه الجرائم، ولو تم التوصل إليه فمن السهل اتلاف الأدلة من قبل الجناة، كما أن هذه الجرائم لا تحدها حدود، فهى جرائم عابرة للحدود مما يثير تحديات ومعوقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش.

11.1. **مرتكبوا الجرائم الالكترونية:**

هناك عدد يقوم بإرتكاب الجرائم الالكترونية وهم (ابراهيم:٢٠١٥، ص٣٦٠-٤٠٣):

طائفة القراصنة' وهي بدورها تنقسم إلى:

القراصنة الهواة(الهاكرز): Hackers يقصد بهم الشباب البالغ المفتون بالمعلوماتية والحاسبات الالية وبعضهم يطلق عليهم صغار نوابغ المعلوماتية واغلبهم من الطلبة. تضم هذه الطائفة الاشخاص الذين يستهدفون من الدخول إلى انظمة الحاسبات الالية غير المصرح لهم بالدخول اليها. كسر الحواجز الامنية الموضوعة لهذا الغرض وذلك بهدف الخبرة أو الفضول.

القراصنة المحترفين :Crackersأعمارهم تتراوح مابين 25–45 سنة في الغالب يكونون ذوي مكانة في المجتمع ودائمًا ما يكونوا من المختصين في مجال التقنية الإلكترونية. هم أكثر خطورة وعادة مايعودون إلى ارتكاب الجريمة مرة أخرى.

طائفة الحاقدين: يطلق عليهم المنتقمون لأنها تنطلق ضد اصحاب العمل والمنشأت التي كانوا يعملون بها وانتقاما من رب العمل وهم أقل خطورة، يرى الباحثون أن أهداف وأغراض الجريمة غير متوفرة لدى هذه الطائفة فهم لا يهدفون إلى اثبات قدراتهم التقنية ومهارتهم الفنية وليبغون تحقيق مكاسب مادية أو سياسية، بل يعمدون إلى إخفاء وإنكار افعالهم واغلب انشطتهم تتم باستخدام تقنيات زراعة الفيروسات والبرامج الضارة لتخريب الأنظمة المعلوماتية.

طائفة المتطرفين الفكريين: يعرف التطرف في هذا المجال بأنه عبارة عن انشطة توظف شبكة الإنترنت في نشر وبث واستقبال وإنشاء المواقع و الخدمات التي تسهل انتقال وترويج المواد الفكرية المغذية للتطرف الفكري، مما دفع بعض المتشددين إلى سلوك الطريق الإجرامي وأصبح هناك ما يعرف بالمجرم المعلوماتي المتطرف الذي يستعمل بما في ذلك للشبكات الاعلامية الاخبارية التي تتبع نشطات الجماعية ونشر بيانات وتصريحات قادتها، وعادة ما يقوم هؤلاء بالاتصال من مقاهي ومكاتب الإنترنت يستعملون كافة المواقع الإلكترونية التي تسعى لتحقيق اغراض دعائية لصالحهم.

طائفة المتجسسون: يقوم هؤلاء بالعبث أو الإتلاف محتويات الشبكة من جانب ومن جانب نخروهو الأهم والذي يشكل الخطر الحقيقي على تلك الواقع على سبيل المثال قد يتم تنزيل الأسرار الصناعية من كمبيوتر في إحدى الشريكات وإرسالها بالبريد الإلكتروني مباشرة إلى منافستها، ومن أهم اهداف هذه الطائفة في استخدام الأنظمة المعلوماتية هي الحصول على معلومات الاعداء والأصدقاء على حد سواء

طائفة مخترقي الأنظمة: يتبادل افراد هذه الطائفة المعلومات فيما بينهم بغية إطلاع بعضهم على مواطن الضعف في الانظمة المعلوماتية وتجري عملية التبادل للمعلومات بينهم بواسطة النشرات الاعلامية الإلكترونية مثل: مجموعات الاخبار، بل ان افراد هذه الطائفة يتولون عقد المؤتمرات لكافة مخترقي الانظمة المعلوماتية بحيث يدعى اليها الخبراء من بينهم للتشاور حول وسائل الاختراق واليات نجاحها.

12.1.**خصائص وسمات مرتكبوا الجرائم الالكترونية:**

يتميز المجرم الالكتروني بعدد من السمات والخصائص التي تجعله مختلفا عن المجرم التقليدى والتي منها (ابراهيم:٢٠١٥، ص٣٦٠-٤٠٣):

- ✓ شخص ذو مهارات فنية عالية متخصص في الجرائم المعلوماتية يستغل مداركه ومهارته في اختراق الشبكات وكسر كلمات المرور والشفرات ويسبح في عالم الشبكات، ليحصل على كل غالي وثمين من البيانات والمعلومات الموجودة في اجهزة الحواسيب من خلال الشبكات.
- ✓ شخص قادر على استخدام خبراته في الاختراق وتغيير المعلومات.
- ✓ شخص قادر على تقليد البرامج أو تحويل اموال.
- ✓ شخص محترف في التعامل مع شبكات الحاسبة.
- ✓ شخص غير عنيف لأن تلك الجريمة لا تلجا للعنف في ارتكابها.
- ✓ شخص يتمتع بذكاء اذ يمكنه التغلب على كثير من العقبات التي تواجهه اثناء ارتكابه الجريمة، حيث يمتلك هذا المجرم من المهارات ما يؤهله للقيام بتعديل وتطوير في الانظمة الامنية حتى لا تستطيع ان تلاحقه وتتبع اعماله الاجرامية من خلال الشبكات أو داخل اجهزة الحواسب فالإجرام المعلوماتي هو اجرام ذكاء.
- ✓ شخص اجتماعي له القدرة على التكيف مع الاخرين.
- ✓ مجرم ذكي: يعتبر الذكاء من أهم صفات المجرم المعلوماتي لأنه يتطلب منه الإلمام التام بتقنية بتكنولوجيا المعلومات والقدرة على تعديل وتغيير برامج الحاسب الآلي.
- ✓ مجرم محترف: يتصف مرتكب الجريمة الالكترونية بأنه على درجة عالية من الخبرة والمهارة في استخدام الحاسب الآلي، والتكنولوجيا الحديثة.
- ✓ مجرم غير عنيف: ينتمي الإجرام الالكتروني في غالبه الأعم إلى إجرام الحيل، وهذا النوع من الإجرام لا يستلزم مقدارا من العنف للقيام به.
- ✓ مجرم متكيف اجتماعيا: فلا يضع المجرم الالكتروني نفسه في حالة عداء مع المجتمع الذي يحيط به، بل إن ذكاءه يدفعه للتكيف مع المجتمع، وكلما ازداد تكيفه مع المجتمع كلما زادت خطورته الإجرامية.
- ✓ الميل إلى ارتكاب الجرائم: يتميز مرتكبو الجرائم الالكترونية بفرط في النزعة الإجرامية والميل إلى ارتكاب الجرائم.
- ✓ الميل إلى التقليد: أغلب الجرائم الالكترونية تتم من خلال محاولة الفرد تقليد غيره بالمهارات الفنية
- ✓ الجريمة وتقنية المعلومات
- ✓ التقنيات كهدف مثلا اختراق أنظمة البنوك والشركات.

- ✓ التقنيات كسلاح مثلا الترويج لأفكار هدامة ضارة بالمجتمع.
- ✓ التقنيات كمساعد مثلا استعمالها في التزوير والتزييف والاحتيال.

13.1.الهجمات الإلكترونية وأشكالها:

وصلت الجرائم الإلكترونية إلى حد القتل؛ ففي شهر 9 من عام 2020، توفيت امرأة في دوسلدورف في أحد المستشفيات الألمانية بعد تعطل نظام الحاسوب بسبب برنامج للقرصنة بواسطة الفدية، وهو برنامج خبيث يقيد الوصول إلى نظام الحاسوب الذي يصيبه. ويعكس هذا الهجوم الإلكتروني مدى هشاشة القطاع الصحي في مواجهة هذه الهجمات. وقال الكاتب أنوش في تقرير نشرته صحيفة لوتون (le temps)السويسرية، إنه لم يحدث أن سُجلت حالات وفاة نتيجة هجوم إلكتروني. ولكن تسبب هجوم سيبراني في وفاة مريضة في مستشفى بدوسلدورف نتيجة عدم تلقيها للعلاج. وأعلنت السلطات الألمانية عن العواقب المأساوية للهجوم السيبراني "الإلكتروني" الذي استهدف الشبكة الإلكترونية للمستشفى الجامعي في دوسلدورف ليصيب أنظمته بالشلل الجزئي منذ 9 سبتمبر/أيلول.

وبرنامج الفدية المعروف باسم "رانسوم وير" هو برنامج ضار يستهدف نقاط الضعف في برامج معينة للسماح للمهاجمين بالتحكم عن بُعد في أنظمة الحاسوب. ومقابل إعادة الوصول إلى الملفات المحملة على أجهزة الحاسوب، عادة ما يطلب المخترق فدية تصل إلى عشرات أو حتى مئات الآلاف من الفرنكات.

-أشكال هجمات الجرائم الإلكترونية:

تتعدد الأمثلة الشهيرة لأنواع وأشكال مختلفة من هجمات الجرائم الإلكترونية التي يستخدمها مجرمو الإنترنت ومنها (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

-هجمات البرمجيات الخبيثة :هجوم البرامج الضارة هو إصابة نظام الكمبيوتر أو الشبكة بفيروس كمبيوتر أو أي نوع آخر من البرامج الضارة، ويمكن لمجرمي الإنترنت استخدام الكمبيوتر الذي تم اختراقه بواسطة البرامج الضارة لعدة أغراض. وتشمل هذه سرقة البيانات السرية، واستخدام الكمبيوتر لتنفيذ أعمال إجرامية أخرى، أو التسبب في إتلاف البيانات.

- التصيد: حملة التصيد الاحتيالي هي عندما يتم إرسال رسائل البريد الإلكتروني العشوائية أو غيرها من أشكال الاتصال بشكل جماعي، بهدف خداع المستلمين للقيام بشيء يقوض أمنهم أو أمن المنظمة التي يعملون بها.

قد تحتوي رسائل حملة التصيد الاحتيالي على مرفقات مصابة أو روابط لمواقع ضارة، أو قد يطلبون من المتلقي الرد بمعلومات سرية. يُعرف نوع آخر من حملات التصيد الاحتيالي باسم التصيد بالرمح، هذه حملات تصيد مستهدفة تحاول خداع أفراد معينين لتعريض أمن المنظمة التي يعملون بها للخطر. على عكس حملات التصيد الجماعي، والتي تكون عامة جداً في الأسلوب، يتم عادةً صياغة رسائل التصيد الاحتيالي بالرمح لتبدو وكأنها رسائل من مصدر موثوق.

-هجمات حجب الخدمة الموزعة :هجمات DoSالموزعة ((DDoSهي نوع من هجمات الجرائم الإلكترونية التي يستخدمها المجرمون الإلكترونيون لإسقاط نظام أو شبكة، تُستخدم أجهزة إنترنت المتصلة أحياناً لشن هجمات .DdoS

يربك هجوم DDoSالنظام عن طريق استخدام أحد بروتوكولات الاتصال القياسية التي يستخدمها لإرسال البريد العشوائي إلى النظام بطلبات الاتصال. قد يستخدم مجرمو الإنترنت الذين يقومون بالابتزاز الإلكتروني تهديد هجوم DDoSللمطالبة بالمال، يمكن استخدام DDoSكتكتيك إلهاء أثناء حدوث نوع آخر من الجرائم الإلكترونية.

2.**الجرائم المتصلة بالجرائم الالكترونية:**

الجرائم التي ترتكب بواسطة استخدام شبكة الانترنت كثيرة ومتنوعة ومنها الواقعة على الأموال ومنها الواقعة على الأشخاص بل كذلك الجرائم الواقعة على الملكيات ومنها حقوق المؤلفات والمخترعات. والى أكثر من ذلك أصبحت الجرائم المستخدمة عن طريق الانترنت أكثر خطورة بدخول الجرائم الماسة بأمن الدولة الداخلي وكذلك الجرائم الماسة بأمن الدولة الخارجي وكذلك الجرائم التي تمس بالمعاهدات أو الجرائم ذات الطبيعة الدولية كالجرائم الإرهابية.

١/٢/١ جريمة القذف والتشهير الالكتروني:

مفهوم السب والقذف والتشهيرعبر الوسائل الالكترونية (ابراهيم:٢٠١٦، ص.٤٤-٦٥)كما يلى :

السب: هو كل من سب غيره علنا بأن وجه إليه ألفاظا تمس شرفه أو كرامته عبر أي وسيلة إلكترونية.

القذف: من أسند لشخص واقعة توجب عقابه قانونا أو تمس شرفه أو كرامته أو تعرض لبغض الناس أو احتقارهم.

التشهير: ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.

أركان جريمة السب و القذف عبر الوسائل الالكترونية (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

اولاً: الركن المادي للجريمة

- الفعل
- النتيجة
- العلاقة السببية

ثانياً: الركن المعنوي

- القصد الجنائي (نية المتهم)

. **الإساءة**: هو وصف عام يشمل المعاملة السيئة والإتيان بالقبيح من القول والفعل. كما تشير إلى إساءة استخدام صلاحيات أو مسؤولية مناط بها شخص ما بالقيام بأعمال مشينة، والتي يعاقب عليها القانون.

التشهير: شكل من أشكال العدالة الأهلية على الإنترنت، يتم فيها إذلال وفضح الأهداف علانية بسبب أفعالهم التي تم عملها في الخفاء، أو دون الرغبة في نشرها على وسائل التواصل.

مخاطر ظاهرة السب والقذف عبر الوسائل الإلكتروني

- الفرع الأول: فضح المجني عليه: أي إظهار المجني عليه أمام العلن بصورة سيئة عبر الوسائل الإلكترونية، سواء عن طريق السب أو القذف بصورة فاضحة على نحو يمكن للجميع رؤية هذه الإساءة او حتى عن طريق تناقلها بالسمع.
- الفرع الثاني: صعوبة محو الإساءة عند التشهير بشخص او فضحة عن طريق إحدى الوسائل الالكترونية لابد من اتخاذ العديد من الإجراءات لمحو هذه الإساءة، بالإضافة إلى اللجوء للسلطات المختصة والخبراء في هذه الأمور لاتخاذ

التدابير والإجراءات اللازمة لعدم تفاقم هذا الضرر والحد منه، ومن ثم اتخاذ الإجراءات اللازمة مع مرتكبها لمعاقبته لما بدر منه من إساءة.

كيفية حماية الأشخاص من جريمة السب والقذف والتشهير عبر الوسائل الالكترونية

- ✓ الوسائل القانونية والجهات التي يجب اللجوء اليها.
- ✓ اللجوء لسلطة الجرائم الالكترونية والجهات المختصة في هذا الشأن
- ✓ عدم رد الإساءة بالإساءة: أي عدم ارتكاب مثل الأفعال المسيئة بهدف رد الفعل لصاحب الفعل ووضعه بنفس الموضع للانتقام منه.
- ✓ عدم الخوف، أي عند التعرض لأي من هذه الأفعال المسيئة عدم الخوف والخضوع لأوامر الجاني

١/٢/٢ جريمة السرقة الالكترونية:

تعرف جريمة السرقة الالكترونية على أنها "هي كل سلوك غير قانوني يتم باستخدام الأجهزة الإلكترونية، ينتج عنها حصول المجرم على فوائد مادية أو معنوية مع تحميل الضحية خسارة مقابلة وغالبا ما يكون هدف هذه الجرائم هو القرصنة من أجل سرقة أو إتلاف المعلومات".

وفي الفقه الجنائي الإسلامي، تعرف السرقة الالكترونية على أنها " هي التي تشمل سرقة المعلومات والبرامج، وسرقة الأموال، باختراق المواقع الالكترونية، والحسابات المصرفية، وبطاقات الائتمان ونحوها". (ابراهيم:٢٠١٦، ص.٤٤-٦٥).

-**سرقة المعلومات** ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطوير التقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها. الخ.

١/٢/٣ جريمة النصب والاحتيال الالكتروني:

مفهوم الاحتيال الإلكتروني الاحتيال الإلكتروني أو التصيد الاحتيالي هو نوع من أنواع الجرائم الإلكترونية الذي يستخدمه مجرمون لاستدراج مستخدم شبكة الإنترنت للكشف عن معلومات شخصية حتى يتمكن هؤلاء المجرمون من استغلالها لصالحهم. ويعرف الاحتيال المالي بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف ..الخ. (ابراهيم:٢٠١٦، ص.٤٤-٦٥).

- أنواع الاحتيال :حدد اتحاد مصارف الإمارات 8 أنواع من الاحتيال، وهي (احتيال خصوصية البيانات-الاحتيال عبر الهاتف- الاحتيال عبر البريد الإلكتروني- احتيال اليانصيب- الاحتيال عبر ماكينة الصراف الآلي- الاحتيال عبر بطاقة الشريحة البديلة- الاحتيال عبر الحبر السري، الاحتيال عبر تحويل الأموال).
- الاحتيال عبر البريد الإلكتروني وكيف يمكن الحماية منه:

هو نوع من الاحتيال حيث يُرسل المحتال رسائل على البريد الإلكتروني تشبه الصادرة من المؤسسات المالية أو غيرها من السلطات، وتتضمن هذه الرسائل تحذيرات بأن الحساب المصرفي للضحية سيُغلق إذا لم يتم توفير معلومات معينة على الفور عبر النقر على رابط متوفر في البريد الإلكتروني.

وفيما يخص الحماية منه يشير الاتحاد إلى ضرورة عدم الرد على المكالمات المجهولة أو غير المرغوب فيها، أو رسائل البريد الإلكتروني أو الرسائل العادية المشبوهة، وإذا ساورتك الشكوك اتصل مباشرة بمصرفك على رقمه المنشور على موقعه الرسمي على الإنترنت، ولا تقدم معلومات مصرفية لأي شخص حتى في حالة ادعاء الشخص المتصل أنه من البنك، ولا تُفصح عن أي معلومات حساسة أو تشاركها مع أي شخص مثل التفاصيل المصرفية ورقم التعريف الشخصي وكلمة المرور لمرة واحدة ومعلومات بطاقة الائتمان، وراجع حسابك المصرفي وبيانات بطاقة الائتمان على فترات منتظمة لاكتشاف أي معاملات مشبوهة، واستخدم فلاتر الأمان الخاصة بتطبيقات وسائل التواصل الاجتماعي لحماية ملفك الشخصي والتأكد من عدم وصول أي شخص إلى بياناتك، ولا تقم بتحميل تطبيقات غير معروفة، وإذا قمت بذلك لا تسمح لها بالوصول إلى الأرقام المسجلة على هاتفك أو الصور أو الوصول إلى ملفات أخرى تطالب بها هذه التطبيقات. (ابراهيم:٢٠١٦، ص.٤٤-٦٥).

- الاحتيال عبر ماكينة الصراف الآلي وكيف يمكن تجنبه

- يحدث الاحتيال عبر الصرّاف الآلي عند نسخ بطاقة الخصم / الائتمان الشخصية عندما يتعامل العميل مع أي ماكينة صرّاف آلي.

وللحماية منه حاول استخدام ماكينة الصرّاف الآلي الموجودة في مبنى البنك بدلاً من ماكينات الصرّاف الآلي المستقلة في الأماكن العامة، وابحث عن أجهزة جديدة / كاميرات / لوحة مفاتيح أو أي لافتات موضوعة بطريقة مشبوهة أو غير معتادة، وتحقق من وجود أي خدوش أو أشرطة لاصقة أو بقايا غراء حول فتحة إدخال البطاقة / لوحة المفاتيح أو إذا كان يمكن إزالة أي من هذه الأجزاء، وابحث عن أي شيء قد يحتوي على فتحة صغيرة أو فتحة للكاميرا تستهدف لوحة المفاتيح، ولا تقم بإدخال بطاقتك حتى يتم طلبها من شاشة العرض، وقم بتغيير رقم التعريف الشخصي الخاص بك بشكل دوري، واشترك في تنبيهات الرسائل القصيرة مع البنك الذي تتعامل معه، وإذا تم التشويش على بطاقتك أو الاحتفاظ بها في ماكينة الصرّاف الآلي، أبلغ البنك بذلك على الفور.

- كيف يمكن الحماية من الاحتيال عبر تحويل الأموال؟

كن حذراً إذا تلقيت بريداً من عميل يبلغك بتغيير تفاصيل بريده الإلكتروني / حسابه المصرفي، كما يُرجى الاتصال بالعميل على رقم هاتفه للتحقق إذا كان قد أرسل هذا البريد الإلكتروني، وتحقق دائماً من جميع الرموز الخاصة بعنوان البريد الإلكتروني، وإذا لم تكن متطابقة اتصل بالعميل للتأكد، وإذا كان البريد الإلكتروني يوجهك إلى إرسال أموال إلى رقم حساب مصرفي دولي مختلف أو حساب آخر، يُرجى الاتصال بالعميل للتأكد، واتصل دائماً على أرقام هواتف عميلك المعروفة فقط وليس على الأرقام المذكورة في رسالة البريد الإلكتروني، وقم بتغيير كلمة المرور الخاصة بك بانتظام وإنشاء كلمات مرور قوية ومركبة وتغييرها بشكل متكرر، ولا تستخدم كلمة المرور نفسها في جميع التطبيقات.

وبالنسبة لحسابات البريد الإلكتروني المختلفة، استخدم كلمة مرور مختلفة ولا تشارك أبداً كلمات المرور الخاصة بك مع أي شخص، واحصل على برنامج مكافحة فيروسات محدث على أجهزة الكمبيوتر لديك لحظر البرامج الضارة / الفيروسات / مفاتيح الولوج، وتصفح الإنترنت بعناية.

- كيف يمكن الاحتيال عبر الهاتف وكيفية الحماية منه؟

يتصل المحتالون بالهاتف الأرضي للضحية أو هاتفه المحمول بصفتهم ممثلين للوكالات الحكومية أو البنوك أو عبر وكالة تسويق معروفة. يجمع المحتالون ملف تعريف رئيسي للضحية عبر تقنيات الهندسة الاجتماعية لإضفاء غطاء شرعي يمكّنهم من مطالبة الضحية بمشاركة بياناتها وإقناعها / خداعها عبر الهاتف لتوفير معلومات شخصية أو تحويل الأموال، لا ترد على المكالمات المجهولة أو غير المرغوب فيها، وإذا تم إبلاغك بوجود إجراء حازم على حسابك المصرفي لا داعي للفزع. اتصل بمركز الاتصال التابع للبنك الخاص بك وتحقق من سلامة حسابك، ولا تنشر رقم هاتفك المحمول وتفاصيل الاتصال الأخرى الهامة بسهولة على وسائل التواصل الاجتماعي أو شبكات التواصل الأخرى، ولا توفر معلوماتك المصرفية لأي شخص حتى إذا كان الشخص المتصل يدعي أنه من البنك، ولا تقبل أبداً أي طلب صداقة على فيسبوك أو لينكد إن أو أي موقع آخر من شخص لا تعرفه (حتى إذا كان لديكم أصدقاء مشتركون)، واستخدم فلاتر الأمان الخاصة بتطبيقات وسائل التواصل الاجتماعي لحماية ملفك الشخصي والتأكد من عدم وصول أي شخص إلى بياناتك

٤/٢/١ جريمة التزوير الالكتروني:

وردت عدة تعريفات لجريمة التزوير الالكتروني وذلك على النحو التالي (خالد :٢٠٠١، ص.٢٢-٣٦):

يعرف التزوير عموما بأنه هو: تغيير الحقيقة بقصد الغش في سند أو وثيقة أو إي محرر أخر بإحدى الطرق المادية والمعنوية التي بينها القانون، تغييراً من شأنه إحداث ضرر بالمصلحة العامة أو بشخص من الأشخاص.

ويعرف التزوير على أنه " هو تغيير الحقيقة في محرر بإحدى الطرق التي وضحها القانون تغييراً من شأنه أن يسبب ضرراً"

والقصد الجنائي الخاص من التزوير كركن من أركان وقوعه وهو تغيير الحقيقة في بيانات محرر ما، بإحدى الطرق المحددة نظاماً، مع ترتيب ضرر للغير ومع توافر نية استعمال المحرر للحصول على منفعة أو قضاء مصلحة من أجلها تمت عملية التزوير.

والتزوير الالكتروني هو أحد أقسام جريمة التزوير ويعني أي تغيير للحقيقة يرد على مخرجات الحاسب الآلي سواء تمثلت في مخرجات ورقية مكتوبة كتلك التي تتم عن طريق الطابعة أو كانت مرسومة عن طريق الراسم ويستوي في المحرر الإلكتروني أن يكون مدوناً باللغة العربية أو لغة أخرى لها دلالتها، كذلك قد يتم في مخرجات ورقية شرط أن تكون محفوظة على دعامة، كبرنامج منسوخ على أسطوانة وشرط أن يكون المحرر الإلكتروني ذا أثر في إثبات حق أو أثر قانوني معين.

ويعرف التزوير الالكتروني بأنه تغيير الحقيقة في المستندات المعالجة آليا والمستندات المعلوماتية وذلك بنية استعمالها.

ويعرف التزوير الإلكتروني إجرائياً بأنه تغيير البيانات والمعلومات في المستندات المعالجة آليا باستخدام أجهزة وبرمجيات اختراق وتعد للحصول على مستندات تحاكي الأصل ولكن مزورة في مضمونها وصيغتها بنية استخدامها في تحقيق مصلحة لمرتكب التزوير أو لشخص آخر.

خصائص جريمة التزوير الإلكتروني:

إن الطابع التقني لهذه الجريمة يضفي عليها عدة خصائص يأتي في مقدمتها توافر القصد الجنائي الخاص (التزوير) سواء في المحرر المعلوماتي أو سجلات الحاسب الآلي عن طريق إدخال بيانات غير صحيحة بسجلات الحاسب ، أو سرقة منظومة التوقيع الإلكتروني واستخدامه بدلاً من صاحبه الأصلي ، مما يشكل اعتداء على النظام المعلوماتي لأن القيام بذلك يتطلب الاختراق والتعدي والدخول على المواقع دون تصريح أو استغلال التصريح في ارتكاب جريمة التزوير بإساءة استغلال الثقة، كما تعد جريمة التزوير الإلكتروني من الجرائم العابرة للحدود الجغرافية التي لا تحتاج لعنف جسدي أو مقاومة كما في الجرائم التقليدية، بل تتطلب حرفية وإتقاناً في التنفيذ وهدفها الرئيسي هو تحقيق الربح المالي ولذلك ترتب عليها إيقاع الضرر بأفراد المجتمع، لذا يتوافر فيها القصد الجنائي.

كما أن جرائم التزوير تحتاج إلى التخطيط والدقة في التنفيذ والمعرفة الفنية باختراق الحواجز الأمنية وتدميرها والوصول إلى المعلومات والبيانات الخاصة بالأفراد أو المنظمات وتغييرها والعبث بها لتحقيق مصالح معينة لمرتكب الجريمة أو لصالح طرف أو أطراف أخرى.

ومن أهم خصائص جريمة التزوير الإلكتروني عدم وجود أثر مادي ظاهر يشير إلى مرتكبيها، فطبيعة هذه الجريمة التي تتكون من ذبذبات ونبضات كهربائية غير مرئية تجعل من الصعب اكتشافها، كما أن سهولة إتلاف الأدلة الإلكترونية يجعل من الصعب تتبع مرتكبيها والقبض عليهم. ويشير العريان (2004، ص. 49) إلى أن صعوبة تتبع مرتكب الجريمة الإلكترونية يعزى إلى سهولة تدمير الأدلة المادية وإتلافها بعد ارتكاب الجريمة.

ويشير مدني إلى أن ارتكاب جريمة التزوير الإلكتروني يتطلب الإلمام بمعارف ومهارات فنية متقدمة في مجال الحاسب الآلي والإنترنت.

خطورة جريمة التزوير الالكتروني (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

1 -أن جريمة التزوير الإلكتروني تؤدي إلى فقدان الثقة بالتعاملات الإلكترونية وبصفة خاصة عند قيام البعض بالاستيلاء على أرقام بطاقات الائتمان أو تحويل المبالغ المالية من أرصدة بعض العملاء إلى أرصدتهم أو الشراء والتسديد من حساباتهم بعد اختراق نظم المعلومات في البنوك مما يفقد العديد الثقة في التعاملات الإلكترونية ويجعلهم يحذرون منها

2 -لا تقتصر على التزوير المادي بل يمكن ارتكابها بطرق التزوير المعنوي جعل واقعة مزورة في صورة واقعة صحيحة – كما في حالة تغيير الغرض من القدوم لأحد القادمين إلى المملكة من قادم إلى الزيارة إلى قادم عمل، أو تغيير مسمى الوظيفة من عسكري إلى متسبب لكي يستطيع السفر بها خارج المملكة دون الحصول على إذن من مرجعه، وهذه الجرائم يتم ارتكابها من قبل المصرح لهم بالدخول على النظام الذين يسيئوون استغلال تلك الثقة أو من قبل خبراء على درجة عالية من الكفاءة في استخدام الحاسب الآلي ولهم خبرة طويلة في استخدام تقنيات الاختراق والتعدي ويتمتعون بقدرات فائقة على إتلاف الأدلة المادية التي تدينهم بعد ارتكاب جرائمهم

من هنا يمكننا أن نقول إن جريمة التزوير الإلكتروني تتميز في مجال المعالجة الآلية للمعلومات بالآتي:

1- مرتكب جريمة التزوير الإلكتروني في الغالب شخص يتميز بالذكاء والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال أنظمة الحاسب الآلي وكيفية تشغيله وكيفية تخزين المعلومات والحصول عليها ، في حين أن مرتكب الجريمة التقليدية في – الغالب - شخص أمي بسيط، متوسط التعليم .

2- مرتكب جريمة التزوير الإلكتروني – في الغالب – يكون متكيفا اجتماعيا وقادرا ماديا ، باعثه من ارتكاب جريمته الرغبة في قهر النظام أكثر من الرغبة في الحصول على الربح أو النفع المادي، في حين أن مرتكب الجريمة التقليدية – غالبا – ما يكون غير متكيف اجتماعيا وباعثه من ارتكابه الجريمة هو النفع المادي السريع .

3- تقع جريمة التزوير الإلكتروني في مجال المعالجة الآلية للمعلومات وتستهدف المعنويات لا الماديات، وهي بالتالي أقل عنفاً وأكثر صعوبة في الإثبات لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه ، وهذا يعسر إجراءات اكتشاف الجريمة ومعرفة مرتكبها ، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا ماديا أو شهادة شهود أو غيرها من أدلة الإثبات، كما أن موضوع التفتيش والضبط قد يتطلب أحيانا امتداده إلى أشخاص آخرين غير المشتبه فيه أو المتهم.

4- جريمة التزوير الإلكتروني ذات بعد دولي، أي أنها عابرة للحدود ، فهي قد تتجاوز الحدود الجغرافية باعتبار أن تنفيذها يتم عبر الشبكة المعلوماتية وهو ما يثير في كثير من الأحيان تحديات قانونية إدارية فنية ، بل وسياسية بشأن مواجهتها لاسيما فيما يتعلق بإجراءات الملاحقة الجنائية.

الوسائل المستخدمة في جريمة التزوير الإلكتروني:

هناك وسائل متعددة تتواكب مع التطور التقني المعاصر، وتسهم في ارتكاب جريمة التزوير الإلكتروني بطرق مبتكرة أحيانا وتقليدية أحيانا، ومنها ما يلي: (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

1-استخدام أدوات كسر كلمات السر، أو برامج فك التشفير وهي عبارة عن أقراص وبرامج تحتوي لوغاريتمات تقوم بعمليات تباديل وتوافيق بسرعات مهولة حتى الحصول على الرقم السري الخاص بالنظام، وإمكانية الدخول عليه واستخدامه، ومن ثم ارتكاب جريمة التزوير

2-إفشاء الرقم السري من قبل الموظف لزملاء العمل بحسن النية، عن طريق المحاولة المتكررة من خلال لوحة المفاتيح، حيث يمكن أن تثمر إحدى هذه المحاولات عن الرقم السري الصحيح الذي يمكن المستخدم من الدخول على النظام والعبث به، وكذلك ارتكاب جريمة التزوير الإلكتروني، وكما أن استخدام أدوات كسر كلمات السر أو برامج فك التشفير من أهم وسائل ارتكاب الجريمة الإلكترونية، بينما تؤكد أهمية تلك البرامج وقدرتها الفائقة على فك أية شفرة.

3-مولدات أرقام البطاقات الائتمانية، حيث تمكن من الحصول على أرقام بطاقات الائتمان الخاصة بأي مودع، ومن ثم القيام بعمليات الشراء باستخدام رصيده بالبنك، بالإضافة إلى إمكانية ارتكاب هذه الجريمة باستخدام الأجهزة ومحركات الأقراص المرنة والليزر بعد اختراق المواقع والعمل على تعديل محتوياتها، أو سرقة منظومة التوقيع الإلكتروني. وكما أن التزوير لا يقتصر على التغيير في سجلات الحاسب الآلي، ولكنه يمتد ليشمل سرقة منظومة التوقيع الإلكتروني

ولا تقتصر وسائل ارتكاب جريمة التزوير الإلكتروني على الطرق السابقة ، بل تشمل وسائل متنوعة من أهمها أدوات التجسس على رزم البيانات أثناء مرورها عبر الشبكة ، ومن خلال الثقوب التي تتخلل بعض البرامج ، وبصفة

خاصة البرامج التي يتم تحميلها من شبكة الإنترنت ، حيث يتعمد المخترقون ترك بعض الثقوب بهذه البرامج واستخدامها كوسيلة للنفاذ إلى نظم المعلومات والعبث بها، أو ارتكاب جرائم التزوير، وكذلك يمكن استخدام الشبكة الواسعة WAN والبرامج المرتبطة بها التي تتيح الفرصة للدخول على بعض المواقع وفك الشفرات الخاصة بها وكذلك الشبكة المحلية LAN وبرامج التشارك في الموارد التي يمكن استخدامها كثغرات للنفاذ إلى بعض المواقع وارتكاب الجرائم الإلكترونية بها . وكما ان تعدد وسائل وأساليب ارتكاب التزوير الإلكتروني باستغلال الشبكات وبعض البرامج المساعدة في اختراق نظم المعلومات والتعدي عليها. كما أنه يمكن استخدام التخفي الشبكي كوسيلة للاختراق والتعدي وارتكاب جريمة التزوير الإلكترونية ، أو من خلال تمويه العنوان الشبكي، للهروب من المسؤولية عند استخدام تقنيات التتبع واسترجاع المعلومات لمعرفة الموقع الذي تم منه الاختراق والتعدي، بجانب لجوء البعض إلى استخدام لواقط ضربات لوحة المفاتيح التي قد تفتح بالمصادفة بعض المواقع المحجوبة وتمكن المخترقين من ارتكاب جرائم التزوير بهذه المواقع ، وأيضا يمكن استخدام شبكة VPN التي تمنح إمكانات واسعة للدخول على المواقع من خلال برامجها التي تستطيع فك تشفير بعض المواقع وإتاحتها للمستخدمين دون قيود، مما يعني أن الانضمام لهذه الشبكة كفيل بحل مشكلة التشفير والمواقع المحجوبة . كما أن هناك إمكانية استخدام الشبكات الخاصة في عمليات الاختراق والتعدي في ضوء ارتباطها بمنظومات خاصة تتغلب على كلمات المرور وتكسرها، وتفك الشفرات وتوفر وقت وجهد المخترقين أثناء محاولات الدخول العشوائي.

١/٢/٥ جريمة الإرهاب الالكتروني:

الإرهاب: مشتق من الفعل أرهب، بمعنى أخاف، وأفزع، يقال: أرهبه رهبه واسترهبه: أخافه وفزعهو استرهب وشاع استعمال لفظة الإرهاب في الاصطلاح المعاصر على الأعمال التخريبية التي تنطوي على قتل، وسفك للدماء، وتخريب للمنشآت العامة والخاصة، بقصد مقاومة السلطات، فضلا عن إرهاب المواطنين، وتخويفهم، وإشاعة حالة من الفوضى والاضطراب في المجتمع (ابراهيم:٢٠١٦، ص.٤٤-٦٥).

أما الإرهاب الإلكتروني فعرفه البعض بأنه: "استخدام التقنيات الرقمية لإخافة وإخضاع الآخرين، أو القيام بمهاجمة نظم المعلومات، على خلفية دوافع سياسية، أو عرقية، أو دينية" ومن المعلوم أن الجريمة الإلكترونية تتطور بتطور المجتمع، وأصبحت أكثر خطورة من الجريمة العادية، لأنها تستخدم عبر فضاء هذا الكون الواسع، ومن أي موقع في العالم، الأمر الذي يصعب من مهمة الدول في مواجهة هذه الجريمة التي تهدد أمن الأفراد، والمؤسسات، والدول.

والإرهاب الإلكتروني لا يحتاج إلى العنف، فضلا عن صعوبة اكتشافه، أو إثباته، وتعدد مجالاته، وتنوع أنشطته وممارساته، فقد يكون الإرهاب موجها إلى الأفراد من خلال التلصص على حساباتهم الشخصية، وسرقة المعلومات الخاصة بهم، الأمر الذي يجعلهم يقعون تحت طائلة الابتزاز من قبل هؤلاء المجرمين. وقد يكون الإرهاب الإلكتروني موجها إلى المؤسسات: شركات، أو وزارات، أو دول، من خلال سرقة بيانات الشركات، أو أرصدتها، أو العبث بالبيانات الموجودة لديها، أو التلصص على بيانات الدول، والتعرف على المعلومات السرية الخاصة بها، الأمر الذي يوقعها تحت طائلة التهديد من أعدائها، وقد يكون الإرهاب الإلكتروني موجها إلى عقول الشباب من خلال تجنيدهم للقيام بعمليات

إرهابية في دول معينة، أو من خلال إنشاء تنظيمات إرهابية، وتجنيد الشباب للالتحاق بهذه الجماعات والانضمام إليها، مستخدمين في كل ذلك كل وسائل التأثير سواء المال، أو الدين، أو غير ذلك من المؤثرات التي ينخدع بها الشباب، وقد يكون الإرهاب الإلكتروني من خلال ما يبث من أفكار مغلوطة وهدامة تعمل على إثارة الفتن والقلاقل في المجتمعات، ونشر الإشاعات الكاذبة التي تحفز المواطنين وتحثهم على السخط على دولهم وحكوماتهم، وتجعلهم ينقمون منهم ليلا ونهارا ويخرجون للثورة على دولهم.

ولاشك أن هذه الظواهر الجديدة تمثل تحديا جديدا للدولة المعاصرة فيما يتعلق بمواجهة الجريمة والحفاظ على أمن المجتمعات، ودعم استقرارها، وهذا يتطلب من الدول تدريب العديد من الكوادر القادرة على مواجهة هذه الجريمة، ووضع أنظمة الحماية اللازمة لحماية أمن الأفراد، والمؤسسات، والمصارف، والبيانات السرية في الدول، كما يتطلب أيضا من الدول العمل على توعية الأفراد، بكيفية حماية الشخص نفسه من خداع مرتكبي هذه الجرائم، وأيضا توعية المؤسسات وتقديم الدعم المادي والمعنوي لها بحيث تكون آمنة على بياناتها، ونظمها، وأموالها .

كما يتطلب هذا الأمر أيضا فيما يتعلق بالشباب الذين يتعرضون للتجنيد من هذه الجماعات العمل بشكل دائم ومستمر على توعية الشباب بهذه المخاطر، وعمل التدابير الاحترازية اللازمة، وأخذ الخطوات الاستباقية لتكون الدول سباقة في التوعية ونشر ثقافة الحماية للشباب وسائر المواطنين، بل ويجب أيضا إنتاج برامج في وسائل الإعلام المختلفة لتوعية المواطنين ضد مخاطر الإرهاب الإلكتروني وكيفية التعامل معه، والحماية منه في شتى الأمور سالفة الذكر، كما يجب على المؤسسات الدينية في الدول العربية والإسلامية توعية الشباب من مخاطر الانغماس في الفكر الإرهابي، وما يخضعون له من محاولات لتجنيدهم، والعمل على تحصين عقولهم بشكل مستمر، حتى يظل الوطن آمنا مستقرا، بمنأى عن عبث العابثين، ويجب أيضا على الدولة بالإضافة إلى ما تقدم وضع التشريعات القانونية اللازمة التي تعالج مثل هذه الجرائم المستحدثة، والعمل على تتبع هؤلاء المجرمين في شتى البقاع، والحيلولة بينهم وبين العبث بمقدرات الأوطان .

إن مواجهة الإرهاب الإلكتروني أشد خطورة من الإرهاب الموجود على الأرض، لذلك يجب على دول العالم التعاون فيما بينها، لمواجهة هذا المارد الأسود الجديد، الذي يهدد البشرية جمعاء، أفرادا، ومؤسسات، ودولا، ولن تنعم البشرية إلا إذا تعاونت الدول فيما بينها، لما فيه خير للإنسان في شتى بقاع المعمورة، على النحو الذي قاله الحق سبحانه وتعالى:"وتعاونوا على البر والتقوى ولا تعاونوا على الإثم والعدوان". ويشمل الإرهاب الإلكتروني جميع المكونات التالية في بيئة تقنية متغيرة والتي تؤثر على فرص الإرهاب ومصادرة، هذه التغيرات تؤثر على تكتيكات الإرهاب وأسلحته وأهدافه ومن التكتيكات الإرهابية ما يعرف بالإرهاب الإلكتروني ويشمل الإرهاب الالكتروني ما يلى: (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

- ✓ تخريب المعلومات وإساءة استخدامها. ويشمل ذلك قواعد المعلومات، المكتبات، تمزيق الكتب، تخريب المعلومات وتحريف المعلومات، تحريف السجلات الرسمية. الخ.
- ✓ سرقة المعلومات ويشمل بيع المعلومات كالبحوث أو الدراسات الهامة أو ذات العلاقة بالتطويرالتقني، أو الصناعي، أو العسكري، أو تخريبها، أو تدميرها. الخ.

- ✓ تزوير المعلومات ويشمل الدخول لقواعد في النظام التعليمي وتغيير المعلومات وتحريفها، مثل تغيير علامات الطلاب.
- ✓ تزييف المعلومات: وتشمل تغيير في المعلومات على وضع غير حقيقي مثل وضع سجلات شهادات لم تصدر عن النظام التعليمي واصدارها.
- ✓ انتهاك الخصوصية ويشمل نشر معلومات ذات طبيعة خاصة عن الأفراد، أو الدخول لحسابات الأفراد الإلكترونية ونشر معلومات عنهم، أو وضع معلومات تخص تاريخ الأفراد ونشرها.
- ✓ التصنت: وتشمل الدخول لقواعد المعلومات وسرقة المحادثات عبر الهاتف.
- ✓ التجسس: ويشمل اعتراض المعلومات ومحاولة معرفة ما يقوم به الأفراد.
- ✓ التشهير: ويشمل استخدام المعلومات الخاصة أو ذات الصلة بالانحراف أو الجريمة ونشرها بشكل القصد منه اغتيال شخصية الأفراد أو الإساءة.
- ✓ السرقة العلمية: الكتب والبحوث العلمية الأكاديمية وخاصة ذات الطبيعة التجريبية والتطبيقية.
- ✓ سرقة الاختراعات وخاصة في المجالات العلمية لاستخدامها أو بيعها.
- ✓ -الدخول غير القانوني للشبكات: بقصد إساءة الاستخدام أو الحصول على منافع من خلال تخريب المعلومات أو التجسس أو سرقة المعلومات.
- ✓ قرصنة البرمجيات: ويشمل النسخ غير القانوني للبرمجيات واستخدامها أو بيعها مرة أخرى.
- ✓ قرصنة البيانات والمعلومات: ويشمل اعتراض البيانات وخطفها بقصد الاستفادة منها وبخاصة أرقام البطاقة الائتمانية وأرقام الحسابات وكلمات الدخول وكلمات السر.
- ✓ خلاعة الأطفال: وتشمل نشر صور خاصة للأطفال "الجنس السياحي" للأطفال خاصة، وللإناث بشكل عام، ونشر الجنس التخيلي Cyber Six على الشبكات.
- ✓ القنابل البريدية وتشمل إرسال فيروسات لتدمير البيانات من خلال رسالة ملغومة إلكترونية
- ✓ الاحتيال المالي: بالبطاقات وهذا ناتج عن استخدام غير شرعي لبطاقات التسوق أو المالية أو الهاتف ..الخ.
- ✓ -سرقة الأرقام والمتاجرة بها وخاصة أرقام الهواتف السرية واستخدامها في الاتصالات الدولية أو أرقام بطاقات الائتمان.
- ✓ التحرش الجنسي ويقصد به المضايقة من الذكور للإناث أو العكس من خلال المراسلة أو المهاتفة، أو المحادثة، أو الملامسة.
- ✓ المطاردة والملاحقة والابتزاز وتشمل ملاحقة الذكور للإناث أو العكس والتتبع بقصد فرض إقامة علاقة ما، وذلك من خلال استخدام البريد الإلكتروني وإرسال الرسائل.

٣-مواجهة الجرائم الالكترونية وطرق إثباتها:

١/٣ الإثبات الشرعي والقانوني للجريمة الالكترونية:

لا شك في أن التجريم والعقاب يعد من أخطر الأمور التشريعية التي تتصل بحرية المواطنين وذلك بسبب خطورة الآثار التى تترتب عليه، ولذلك فإن النصوص التشريعية التي تصدر به، يتعين أن تصدر دائما وفقاً لمبدأ الشرعية الجنائية والقانونية. الذي نحاول فيما يأتي إلقاء الضوء على الإثبات الشرعى والقانونى للجريمة الإلكترونية كما يلى: (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

أولاً: دستورية الشرعية الجنائية والقانونية للجريمة الالكترونية: تعد الدولة القاسم المشترك بين القانون الدستوري والقانون الجنائي، فالدستور ينظم نشاط الدولة من الناحية السياسية، والقانون الجنائي ينظم نشاطها من الناحية الجنائية من خلال تنظيم علاقة الفرد بالدولة، وعلاقة الأفراد بعضهم مع بعض، ومن مظاهر الصلة ما تتضمنه الدساتير من نصوص ذات صبغة جنائية بدافع الرغبة في فرض حماية الدستور وإسباغه بطابع القدسية عليها لتعلقها بحقوق الأفراد وحرياتهم، فالعلاقة وثيقة بين القانون الدستوري والقانون الجنائي ؛ ذلك أن مبادىء الدستور تسهم في تحديد مضمون القانون الجنائي ذاته بحيث يتوقف تحديد الجرائم على تطوير المبادىء الدستورية أكثر من اعتماده على تطوير القيم والمصالح الاجتماعية، وفي ضوء ذلك يؤدي القانون الجنائي وظيفته في الدولة في إطار الشرعية الدستورية على النحو الذي يحدده الدستور. وقد قام القانون الجنائي على عدد من المبادىء الدستورية، والتي يعد أهمها هو "مبدأ الشرعية الجنائية. الذي يمثل حجر الزاوية للنظام الجنائي بأسره، فمنه تتفرع وحوله تدور كافة المبادئ التي تحكم القواعد الجنائية موضوعية كانت أو اجرائية. ويقصد به بصفة عامة" أن التشريع هو المصدر الأساسي للتجريم والعقاب، وأن السلطة التشريعية هي وحدها المختصة بتحديد الجرائم والعقوبات دون السلطتين القضائية والتنفيذية، وأن القاضي مهمته تطبيق النصوص التي وضعها المشرع. ويرجع تاريخ هذا المبدأ في القانون الوضعي إلى تاريخ الفصل بين سلطات الدولة؛ إذ قبل ذلك كان للملك وحده سلطة تجريم الأفعال بمطلق إرادته. ثم انتقل الأمر في القرون الوسطى للقضاة فكان القضاة يملكون سلطة تحكمية في تجريم الأفعال والعقاب عليها دون نص في القانون، حتى نص على ذلك المبدأ بداية من صدور ميثاق هنري الأول في انجلترا، ثم دستور كلاريندون ، وأكد عليه العهد الأعظم ، وجاءت الثورة الفرنسية لتؤكد عليه في المادة الثانية من إعلان حقوق الإنسان والمواطن الصادر عام 1789، ثم جاء الإعلان العالمى لحقوق الإنسان الصادر عام 1948 ليؤكد عليه ، وتضمنته الاتفاقية الأوربية لحقوق الإنسان الصادرة عام 1950 ، وكذلك العهد الدولي للحقوق المدنية والسياسية لعام1966. ومن هنا يعد هذا المبدأ من المبادىء الدستورية ذات الطابع العالمي، ويرجع الفضل في ظهوره للنور إلى الفقيه الإيطالي " شيزاري دي بكاريا" صاحب الكتاب الشهير" الجرائم والعقوبات" الذي أصدره في سنة 1764، وقد جاء فيه أن" القوانين وحدها هي التى تحدد العقوبات التى تقابل الجرائم..."،"....ولا يستطيع القاضي أن يوقع سواها.

أكدت على ضمانات تطبيق مبدأ الشرعية الجنائية فقضت بأن" النطاق الحقيقي لمبدأ شرعية الجرائم والعقوبات، إنما يتحدد على ضوء ضمانتين تكفلان الأغراض التي توخاها (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

أولهما: أن تصاغ النصوص العقابية بطريقة واضحة محددة لا خفاء فيها أو غموض، فلا تكون هذه النصوص شباكاً أو شراكاً يلقيها المشرع متصيدا باتساعها أو بخفائها من يقعون تحتها أو يخطئون مواقعها، وهي بعد ضمان غايتها أن يكون المخاطبون بالنصوص العقابية على بينة من حقيقتها، فلا يكون سلوكهم مجافٍ لها بل متسقا معها.

وثانيهما: ومفترضها أن المرحلة الزمنية التى تقع بين دخول القانون الجنائي حيز التنفيذ وإلغاء هذا القانون، إنما تمثل تلك الفترة التى كان يحيا خلالها، فلا يطبق على أفعال أتاها جناتها قبل نفاذه، بل يتعين أن يكون هذا القانون سابقا عليها فلا يكون رجعيا. أكدت على حدود تفسير القاضي للنص الجنائي بقضائها بأن" لا يجوز إعمال نصوص عقابية يسيء تطبيقها إلى مركز قائم لمتهم، ولا تفسيرها بما يخرجها عن معناها أو مقاصدها، ولا مد نطاق التجريم – وبطريق القياس-إلى أفعال لم يؤثمها القاضي من بينها ما يكون أكثر ضمانا للحرية الشخصية في إطار علاقة منطقية يقيمها بين هذه النصوص وإرادة المشرع، سواء في ذلك تلك التي أعلنتها، أو التي يمكن افتراضها عقلاً.

ثانياً-مبررات مبدأ الشرعية الجنائية والقانونية للجريمة الالكترونية (ابراهيم:٢٠١٦، ص.٤٤-٦٥):

-تحقيق مبدأ العدالة: فاحترام الذات الإنسانية يتطلب حصر الأفعال غير المشروعة الكترونيا في صورة جرائم الكترونية، وأن تتحدد تحديدا دقيقا العقوبات التى عن طريقها يواجه الشارع هذه الجرائم وأن يتم إعلام المجتمع جميعا بهذه الجرائم والعقوبات.

-تحقيق مبدأ الفصل بين السلطات: فهناك سلطة ممثلة من الشعب تتولى وضع نصوص التجريم والعقاب بالنسبة للجرائم الالكترونية، وهناك سلطة قضائية تتولى تطبيق هذه النصوص ثم هناك سلطة تنفيذية تتولى تنفيذ ما يصدر عن السلطة القضائية من أحكام في هذا الشأن.

تحقيق مبدأ الردع العقابي: ذلك عن طريق إعلام المخاطبين بالقانون بنصوص التجريم والعقاب المقررة للجرائم الالكترونية ومضمونها والعقوبات المقررة لها، مما يؤدي إلى إحجامهم عن إرتكاب الجريمة مخافة الحكم عليهم بهذه العقوبة، كما يؤدي باقتناع مرتكب الجريمة الالكترونية بالعقوبة المطبقة عليه.

تحقيق مبدأ المساواة في العقاب: فالنصوص الخاصة بالتجريم والعقاب للجرائم الالكترونية تصاغ بشكل عام ومجرد بحيث تطبق على الكافة، بل وعلى جميع الوقائع دون تمييز، وهذا سيؤدى إلى تحقيق المساواة بين الأفراد أمام القانون فلا يختلف تطبيق القانون على حسب الوضع الاجتماعي أو صفة الجاني.

ثالثاً-نتائج مبدأ الشرعية الجنائية والقانونية للجريمة الالكترونية:

بالنسبة للمشرع: تختص السلطة التشريعية وحدها بمهمة التشريع الجنائي للجرائم الالكترونية، وتلتزم عند وضعها للنصوص الجنائية ألا تتعسف في استعمال حقها في التجريم، بحيث لا يجرم المشرع إلا الأفعال الالكترونية التي تمثل اعتداء على المصالح الأساسية للأمة، وإن كان من الصعب تحديد المصالح الأساسية للأمة التي يقوم عليها بنيان المجتمع ، إلا أنه يكفي في هذا السياق ألا يقوم المشرع الجنائي بحماية مصالح لا تشكل قيمة لدى المجتمع أو لدى أغلب أفراده. ، والنص على عدم سريان نصوص تجريم الجرائم الالكترونية على الوقائع الحادثة قبل صدور نصوص التجريم، بل يقتصر سريانها على المستقبل وهو ما يمكن أن يعبر عنه بمبدأ عدم رجعية النصوص الجنائية للجريمة الالكترونية ،

كما يجب على المشرع الجنائي التزام الوضوح التام في النصوص الجنائية، فلا يجوز أن يلجأ عند إقراره لنصوص التجريم الالكترونى إلى أسلوب " النماذج المفتوحة" باستخدام عبارات غامضة أو حمالة أوجه.

رابعا: الشرعية الجنائية والقانونية للجريمة الالكترونية في مصر (عباس: ٢٠١٥، ص.١-٢٥٤).

علي الرغم من أن المادة 31 من الدستور المصري الصادر عام 2014 جاءت نصا دستوريا صريحا يشير إلى وجوب الحفاظ على المعلومات والبيانات الالكترونية ؛ إذ جرى نصها علي أن" أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة بإتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون"؛ إلا أنه حتى الآن لا يوجد بمصر تشريع عقابي متكامل خاص بالجرائم الالكترونية، كل ما هناك أنه توجد بعض النصوص القانونية المتناثرة في قوانين مختلفة تتحدث عن بعض العقوبات المرتبطة ببعض الجرائم الالكترونية منها قانون الاحوال المدنية المصري رقم 143 لسنة 1994 والذي نظم في عدد من مواده تجريم تعديل بيانات الأحوال الشخصية للمواطنين المسجلة على الحاسب الآلي أو الوسائط الالكترونية الموجودة بمصلحة الأحوال المدنية التابعة لوزارة الداخلية بالتزوير أو الاتلاف أو الاطلاع عليها دون وجه حق، وذلك في عدد من المواد منها المادة 72 من القانون والتى جاءت تنص على أن" فى تطبيق أحكام هذا القانون وقانون العقوبات تعتبر البيانات المسجلة بالحاسبات الآلية وملحقاتها بمراكز معلومات الأحوال المدنية ومحطات الإصدار الخاصة بها المستخدمة في إصدار الوثائق وبطاقات تحقيق الشخصية بيانات واردة في محررات رسمية .فإذا وقع تزوير في المحررات السابقة أو في غيرها من المحررات الرسمية ، تكون العقوبة الأشغال الشاقة المؤقتة أو السجن لمدة لا تقل عن خمس سنوات"، والمادة 74 من القانون والتي جاء في نصها" مع عدم الإخلال بأية عقوبة شديدة منصوص عليها في قانون العقوبات أو في غيره من القوانين،كأن يعاقب بالحبس مدة لا تجاوز ستة أشهر وبغرامة لا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من اطلع أو شرع في الاطلاع أو حصل أو شرع في الحصول على البيانات أو المعلومات التي تحتويها السجلات أو الحاسبات الآلية أو وسائط التخزين الملحقة بها أو قام بتغييرها بالإضافة أو بالحذف أو بالإلغاء أو بالتدمير أو بالمساس بها بأي صورة من الصور أو أذاعها أو أفشاها في غير الأحوال التي نص عليها القانون ووفقا للإجراءات المنصوص عليها فيه ، فإذا وقعت الجريمة على البيانات أو المعلومات أو الإحصاءات المجمعة تكون العقوبة السجن"، و المادة 75 من القانون التي تنص على أنه" يعاقب بالحبس مدة لا تجاوز ستة أشهر وغرامة لا تقل عن مائتي جنيه ولا تزيد على خمسمائة جنيه أو بإحدى هاتين العقوبتين كل من عطل أو أتلف الشبكة الناقلة لمعلومات الأحوال المدنية، أو جزءا منها وكان ذلك ناشئا عن إهماله أو رعونته أو عدم احترازه أو عدم مراعاته للقوانين واللوائح والأنظمة .فإذا وقع الفعل عمدا تكون العقوبة السجن مع عدم الإخلال بحق التعويض فى الحالتين"، اما المادة 76 من القانون فتصرح بأنه "يعاقب بالأشغال الشاقة المؤقتة كل من اخترق أو حاول اختراق سرية البيانات أو المعلومات أو الإحصاءات المجمعة بأية صورة من الصور وتكون العقوبة الأشغال الشاقة المؤبدة إذا وقعت الجريمة فى زمن الحرب".وقد قرر قانون حماية الملكية الفكرية رقم 82 لسنة 2002 في بعض مواده حماية السرقات الأدبية عبر شبكة الإنترنت فجاء نص المادة 140 منه للحديث عن نوعية من جرائم الإنترنت فنص على أنه" تتمتع بحماية هذا القانون حقوق المؤلفين على مصنفاتهم الأدبية والفنية، وبوجه خاص المصنفات الآتية: الكتب والكتيبات والمقالات والنشرات من الحاسب الآلي أو من غيره. من برامج الحاسب الآلي وقواعد

البيانات سواء أكانت مقروءة من الحاسب الآلي أو من غيره من المحاضرات، والخطب، والمواعظ، وأية مصنفات شفوية أخرى إذا كانت مسجلة.....". وجاء نص المادة 181 من القانون ناصا على العقوبة وجرى على أن" مع عدم الإخلال في أية عقوبة أشد في أي قانون آخر، يعاقب بالحبس مدة لا تقل عن شهر وبغرامة لا تقل عن خمسة آلف جنيه ولا تجاوز عشرة آلاف جنيه أو بإحدى هاتين العقوبتين، وكل من أرتكب أحد الأفعال الآتية (نائلة :٢٠٠٤،ص.٣٢):

إذاعي أو أداء محمي طبقاً لأحكام هذا القانون عبر أجهزة الحاسب الآلي أو شبكات الإنترنت أو شبكات المعلومات أو شبكات الاتصال أو غيرها من الوسائل دون إذن كتابي مسبق من المؤلف أو صاحب لحق المجاور.

والإزالة أو التعطيل أو التعييب بسوء نية بأية حماية تقنية يستخدمها المؤلف أو صاحب الحق المجاور كالتشفير أو غيره. وفي حالة العود تكون العقوبة الحبس مدة لا تقل عن ثلاثة أشهر والغرامة التي لا تقل عن عشرة آلاف جنيه ولا تجاوز خمسين آلف جنيه. وفي جميع الأحوال تقضي لمحكمة بمصادرة النسخ محل الجريمة أو المتحصلة منها وكذلك المعدات والأدوات المستخدمة في ارتكابها. ويجوز للمحكمة عند الحكم بالإدانة أن تقضي بغلق المنشأة التي استغلها المحكوم عليه في ارتكاب الجريمة مدة لا تزيد عن ستة أشهر، ويكون الغلق وجوبيا في حالة العود في الجرائم المنصوص عليها في البندين ثانياً وثالثاً من هذه لمادة. وتقضي المنشأة بنشر ملخص الحكم بالإدانة في جريدة يومية أو أكثر على نفقة المحكوم عليه".

كما نظم قانون تنظيم الاتصالات 10 لسنة 2003 بعض جرائم الإنترنت فنص في المادة 73 منه على أن" يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية:

- ✓ إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانونى فى ذلك.
- ✓ إخفاء أو تغيير أو إعاقة أو تحوير أية رسالة اتصالات أو لجزء منها تكون قد وصلت إليه.
- ✓ الامتناع عمداً عن إرسال رسالة اتصالات بعد تكليفه بإرسالها.
- ✓ إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات وذلك دون وجه حق"، كما نص المادة 75 منه على أن" يعاقب بالحبس وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائه ألف جنيه أو بإحدى هاتين العقوبتين، كل من قام بإفشاء أو نشر أو إذاعة أية معلومات حصل عليها بحكم وظيفته أو بسببها عن منشأة عاملة فى مجال الاتصالات متى كان من شأن ذلك أن يؤدى إلى قيام منافسة غير مشروعة بين المنشآت العاملة فى هذا المجال".

وقد جاء قانون التوقيع الالكتروني15 لسنة 2004 لينظم بعض صور الجرائم الالكترونية فنص في المادة 23 منه على أنه " مع عدم الإخلال بأية عقوبة اشد منصوص عليها في قانون العقوبات أو في أي قانون آخر، يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه ولا تجاوز مائة ألف جنيه أو بإحدى هاتين العقوبتين كل من:

(أ) أصدر شهادة تصديق الكتروني دون الحصول على ترخيص بمزاولة النشاط من الهيئة.

(ب) أتلف أو عيّب توقيعا أو وسيطا أو محررا الكترونيا، أو زوّر شيئا من ذلك بطريق الاصطناع أو التعديل أو التحوير أو بأي طريق آخر.

(ج) استعمل توقيعا أو وسيطا أو محررا الكترونيا معيبا أو مزورا مع علمه بذلك.

(د) خالف أيّا من أحكام المادتين (19)، (21) من هذا القانون.

(هـ) توصّل بأية وسيلة إلى الحصول بغير حق على توقيع أو وسيط أو محرر الكتروني او اخترق هذا الوسيط أو اعترضه أو عطله عن أداء وظيفته، وتكون العقوبة على مخالفة المادة(13) من هذا القانون، الغرامة التي لا تقل عن خمسة آلاف جنيه ولا تجاوز خمسين ألف جنيه. وفي حالة العود تزاد بمقدار المثل المقررة، العقوبة المقررة لهذه الجرائم في حديها الأدنى والأقصى. وفي جميع الأحوال يحكم نشر حكم الإدانة في جريدتين يوميتين واسعتي الانتشار، وعلى شبكات المعلومات الالكترونية المفتوحة على نفقة المحكوم عليه".

كما تناول قانون الطفل المعدل بالقانون رقم 126 لسنة 2008 في المادة 116 مكرر أ منه الاستغلال الجنسي للأطفال عبر شبكة الإنترنت والذي جاء نصها" يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن عشرة آلاف جنيه، ولا تجاوز خمسين ألف جنيه كل من استورد أو صدر أو أنتج أو أعد أو عرض أو طبع أو روج أو حاز أو بث أي أعمال إباحية يشارك فيها أطفال أو تتعلق بالاستغلال الجنسي للطفل، ويحكم بمصادرة الأدوات والآلات المستخدمة في ارتكاب الجريمة والأموال المتحصلة منها، وغلق الأماكن محل ارتكابها مدة لا تقل عن ستة أشهر، وذلك كله مع عدم الإخلال بحقوق الغير حسن النية. في قانون آخر، يعاقب بذات العقوبة كل من:

استخدم الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لإعداد أو لحفظ أو لمعالجة أو لعرض أو لطابعة أو لنشر أو لترويج أنشطة أو أعمال إباحية تتعلق بتحريض الأطفال أو استغلالهم في الدعارة والأعمال الإباحية أو التشهير بهم أو بيعهم.

استخدام الحاسب الآلي أو الإنترنت أو شبكات المعلومات أو الرسوم المتحركة لتحريض الأطفال على الإنحراف أو لتسخيرهم في ارتكاب جريمة أو على القيام بأنشطة أو أعمال غير مشروعة أو منافية للأداب، ولو لم تقع الجريمة فعلاً.

ويتضح من العرض السابق أنه لا يوجد في مصر حتى الأن قانون خاص بالجرائم الالكترونية فيما عدا ما سبق توضيحه. وبعض النصوص الواردة في قانون العقوبات خاصة بالجرائم التقليدية يمكن تطويعها بعيدا عن التفسير الضيق لتشمل بعض جرائم الحاسب الآلي، إلا أن هذه النصوص لا زالت ة عن إيجاد التأمين الكافي للمجتمع ضد الأشكال المختلفة للجريمة الالكترونية.

٢/٣ طرق مواجهة الجرائم الالكترونية (الحلول التشريعية والقانونية للجرائم الإلكترونية):

وأمام هذه المشكلة التى تواجه جميع دول العالم الآن نجد أن معظم الدول سلكت إحدى ثلاث طرق لمواجهة الجريمة الالكترونية وهي(نائلة :٢٠٠٤، ص.٣٢):

الطريق الأول-وضع نصوص تشريعية لمواجهة الجرائم الالكترونية:

قلبت الجريمة الإلكترونية العديد من المفاهيم القانونية السائدة سواء، مما يتعين القول معه بأن الإجرام المعلوماتي قد أحدث ثورة في فلسفة التجريم والعقاب والإجراءات الجنائية و ذا كان البحث في مسألة قدرة القواعد الإجرائية التقليدية في ضبط الجريمة الإلكترونية أمرا صعبا فإن الصعوبة تنطلق من إعطاء مفهوم للجريمة الإلكترونية

ذاتها ، لذلك يذهب معظم المهتمين إلى القول بأن الجريمة الإلكترونية باعتبارها مظهرا جديدا من مظاهر السلوك الإجرامي لا يمكن تصورها إلا من خلال ثلاث مظاهر، إما أن تتجسد في شكل جريمة تقليدية يتم اقترافها بوسائل إلكترونية أو معلوماتية، أو في شكل استهداف للوسائل المعلوماتية ذاتها و على رأسها قاعدة المعطيات والبيانات أو البرامج المعلوماتية ، أو أن يتم اقتراف الجرائم العادية في بيئة إلكترونية كما هو الأمر بالنسبة لجرائم الصحافة . فلقد أثارت هذه الجريمة بعض التحديات القانونية والعملية أمام الأجهزة المعنية بالبحث عن الجرائم وضبطها وخصوصا فيما يخص مباشرة إجراءات البحث والتحري التقليدية في بيئة افتراضية لا مكان فيها للأدلة المادية، مما أظهر مدى الحاجة إلى تطوير آليات البحث بما يتلاءم وخصوصيات هذه الجرائم، وجعل مسألة ملاءمة الإجراءات الجنائية في البحث والتحري مع خصوصية الجريمة الإلكترونية تستأثر بإهتمام المشرعين في مختلف الدول. كما أن الجريمة الإلكترونية خلقت عالما جديدا لا يعترف بالحدود الجغرافية والسياسية للدول ولا بسيادتها، حيث فقدت الحدود الجغرافية كل آثر لها في بيئة إلكترونية متشعبة العلاقات، الأمر الذي خلق صعوبات وإشكالات قانونية لا تقتصر على ضبط هذه الجرائم وإثباتها فحسب، وإنما أثارت أيضا تحديات أكثر تعقيدا مرتبطة بتحديد جهة الإختصاص وبالتبعية القانون الواجب التطبيق على هذا الصنف من الجرائم.

الطريق الثانى-وضع الحلول التشريعية. والقانونية للجرائم الإلكترونية(نائلة :٢٠٠٤، ص.٣٢):

أولاً: الحلول التشريعية قصيرة المدى

- ✓ قيام السلطات بإصدار مراسم تنظيمية لمداخل الإنترنت دون أن يكون هناك احتكار للمعلومات، مع ضرورة فرض إجراءات ذات عجلة على مقاهي ومداخل الإنترنت
- ✓ القيام بوضع برامج تساهم في منع الدخول على المواقع المخلّة بالآداب العامة، أو التي تتعارض مع عادات وتقاليد المجتمع التي يعيش فيها، أو ظهور المواقع الإباحية أو الإرهابية حيث كان ظهورها مرتبط بغياب التربية السليمة.
- ✓ ضرورة وضع تدابير عاجلة على حرية المعلومات.
- ✓ العمل على وضع برامج تساهم في الحماية من الفيروسات، وبالتالي يتم وضع مراسيم تنظيمية من شأنها تخفيض أسعار هذه البرامج.
- ✓ وضع خطط تفصيلية تتضمن توعية قانونية، مع التركيز على أهمية التعريف بمدى خطورة الجرائم الإلكترونية. العمل على إصدار مراسيم تساهم في تنظيم عمل الشرطة والقضاء على التقنية المعلوماتية، بالإضافة إلى المحققين وتعريفهم بماهيّة الجرائم الإلكترونية وجرائم الإنترنت.
- ✓ فرض غرامات مالية على أشخاص ومقاهي الإنترنت، في حال سمحت للأفراد بالدخول إلى المواقع المخلّة

ثانياً: الحلول التشريعة طويلة المدى:

- ✓ هنا يتم فرض عقوبات على الجرائم الإلكترونية وضرورة استحداثها بشكل مستمر؛ نتيجة للطابع اللامادي والافتراضي لشبكة الإنترنت.
- ✓ ضرورة وضع نصوص قانونية تكون متناسبة مع التطورات الحالية.
- ✓ القانون التجاري.

الطريق الثالث: الحماية الشخصية لجهاز الحاسب الآلي الشخصي من الجرائم الإلكترونية

من أفضل الطرق لحماية جهاز الكمبيوتر الشخصى وحماية البيانات الشخصية ما يلي:

- ✓ المحافظة على تحديث البرنامج ونظام التشغيل، حيث يضمن تحديث البرامج ونظام التشغيل لديك الاستفادة من أحدث تصحيحات الأمان لحماية جهاز الكمبيوتر الخاص بك.
- ✓ استخدام برامج مكافحة الفيروسات وتحديثها باستمرار: يعد استخدام برنامج مكافحة الفيروسات أو حل شامل لأمن الإنترنت، طريقة ذكية لحماية نظامك من الهجمات. يسمح لك برنامج مكافحة الفيروسات بفحص التهديدات واكتشافها وإزالتها قبل أن تصبح مشكلة، يساعد وجود هذه الحماية في حماية جهاز الكمبيوتر الخاص بك وبياناتك من الجرائم الإلكترونية، ما يمنحك راحة البال.إذا كنت تستخدم برنامجاً لمكافحة الفيروسات، فتأكد من تحديثه باستمرار للحصول على أفضل مستوى من الحماية.
- ✓ -استخدم كلمات مرور قوية :تأكد من استخدام كلمات مرور قوية لن يخمنها الناس ولا تسجلها في أي مكان، أو استخدم مدير كلمات مرور حسن السمعة لإنشاء كلمات مرور قوية بشكل عشوائي لتسهيل ذلك.
- ✓ لا تفتح المرفقات تتمثل الطريقة التقليدية لإصابة أجهزة الكمبيوتر بهجمات البرامج الضارة وأشكال أخرى من الجرائم الإلكترونية عبر مرفقات البريد الإلكتروني في رسائل البريد الإلكتروني العشوائية، لا تفتح أبداً مرفقاً من مرسل لا تعرفه.
- ✓ لا تنقر على الروابط الموجودة في رسائل البريد الإلكتروني العشوائية أو مواقع الويب غير الموثوق بها.
- ✓ هناك طريقة أخرى يصبح بها الأشخاص ضحايا للجرائم الإلكترونية، وهي النقر على الروابط الموجودة في رسائل البريد الإلكتروني العشوائية أو الرسائل الأخرى، أو مواقع الويب غير المألوفة، تجنّب القيام بذلك للبقاء آمناً على الإنترنت.
- ✓ لا تعط معلومات شخصية ما لم تكن آمنة
- ✓ لا تقم أبداً بإعطاء البيانات الشخصية عبر الهاتف أو عبر البريد الإلكتروني ما لم تكن متأكداً تماماً من أمان الخط أو البريد الإلكتروني، وتأكد من أنك تتحدث إلى الشخص الذي تعتقد أنك عليه.
- ✓ الاتصال بالشركات مباشرة بخصوص الطلبات المشبوهة إذا طُلب منك بيانات من شركة اتصلت بك، أغلق المكالمة، اتصل بهم مرة أخرى باستخدام الرقم الموجود على موقع الويب الرسمي الخاص بهم للتأكد من أنك تتحدث معهم وليس مجرماً إلكترونياً.
- ✓ ضع في اعتبارك عناوين URLلمواقع الويب التي تزورها راقب عناوين URLالتي تنقر عليها، هل تبدو شرعية؟ تجنّب النقر على الروابط التي تحتوي على عناوين URLغير مألوفة أو غير مرغوب فيها.
- ✓ إذا كان منتج أمان الإنترنت الخاص بك يتضمن وظائف لتأمين المعاملات عبر الإنترنت، فتأكد من تمكينها قبل إجراء المعاملات المالية عبر الإنترنت.
- ✓ راقب كشف حسابك المصرفي: راقب كشف حسابك المصرفي واستفسر عن أي معاملات غير مألوفة عن طريق بطاقات الائتمان مع البنك، يمكن للبنك التحقيق فيما إذا كانت احتيالية.

وهناك أيضا عدد من الطرق التى من خلالها يمكن مواجهة الجرائم الالكترونية ومنها:(نائلة :٢٠٠٤، ص.٣٢)
محاربة الجريمة الإلكترونية تحتاج لوقفة طويلة وقوية من قبل الدول والأفراد الكل مسؤول عن الإسهام قدر الإمكان لمحاربة والتصدي لها.

تتجسد أول طرق مكافحة الجرائم الإلكترونية عبر الإنترنت في الاستدلال الذي يتضمن كل من التفتيش والمعاينة والخبرة والتي تعود إلى خصوصية الجريمة الإلكترونية عبر الإنترنت، اما الثاني سبل مكافحة الجريمة الإلكترونية هي تلك الجهود الدولية والداخلية لتجسيد قانونية للوقاية من هذه الجريمة المستحدثة، فأما الدولية فتتمثل في جهود الهيئات والمنظمات الدولية والتي تتمثل في:

- ✓ توعية الناس لمفهوم الجريمة الإلكترونية وانه الخطر القائم ويجب مواجهته والحرص على ألا يقعوا ضحية له.
- ✓ ضرورة التأكد من العناوين الإلكترونية التي تتطلب معلومات سرية خاصة كبطاقة ائتمانية أو حساب بنكي.
- ✓ عدم الإفصاح عن كلمة السر لأي شخص والحرص على تحديثها بشكل دوري واختيار كلمات سر غير مألوفة.
- ✓ عدم حفظ الصور الشخصية في الكمبيوتر.
- ✓ عدم تنزيل اي ملف أو برنامج من مصادر غير معروفة.
- ✓ الحرص على تحديث انظمة الحماية مثل: استخدام برامج الحماية مثل نورتون norton، كاسبر سكي، مكافيMcafee....الخ.
- ✓ تكوين منظمة لمكافحة الجريمة الإلكترونية.
- ✓ ابلاغ الجهات المختصة في حال تعرض لجريمة إلكترونية.
- ✓ تتبع تطورات الجريمة الإلكترونية وتطوير الرسائل والأجهزة والتشريعات لمكافحتها.
- ✓ تطوير برمجيات امنة ونظم تشغيل قوية التي تحد من الاختراقات الإلكترونية وبرمجيات الفيروسات وبرامج التجسس مثل مضادات التجسس وهي برامج تقوم بمسح الحاسب للبحث عن مكونات التجسس وإلغائها مثل: lava soft

٣/٣ شروط وطرق الإثبات الالكتروني:

فيما يلى وسائل وطرق الإثبات الإلكتروني للجرائم الإلكترونية(نائلة :٢٠٠٤،ص.٣٢):

يمكن إثبات الجرائم الإلكترونية بواسطة وسائل الإثبات التقليدية غير أن التطور التكنولوجي أدى إلى ظهور وسائل إثبات جديدة.

وسائل الإثبات التقليدية للجرائم الإلكترونية:

وهي تتمثل في الإقرار والشهادة والمعاينة والتفتيش والحجز والاختبار.

1-الإقرار: يعرف الإقرار بأنه إقرار المتهم على نفسه بارتكاب الوقائع المكونة الجريمة كلها أو بعضها من خلال إقرار المتهم بكل أو ببعض الوقائع المنسوبة إليه. والإقرار في الجريمة الإلكترونية لا يختلف في ماهيته عن الجريمة التقليدية. وهو يخضع في اعتماده كوسيلة إثبات لتقدير القاضي.

2-الشهادة: الشهادة هي إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص عما شاهده أو سمعه أو أدركه لحواسه من هذه الواقعة بطريقة مباشرة. والشهادة في مجال الجريمة الإلكترونية لا تختلف من حيث ماهيتها عنها في الجريمة التقليدية. والشاهد في الجريمة الإلكترونية هو ذلك الشخص الفني صاحب الخبرة والتخصص في تقنية وعلوم الحاسب الآلي والذي تكون لديه معلومات جوهرية وهامة للدخول في نظام المعالجة الآلية للبيانات. ويطلق على هذا الشاهد إسم الشاهد المعلوماتي وذلك تمييزا له عن الشاهد التقليدي.

والشاهد المعلوماتي قد يكون إما:

- **مشغلو الحاسوب الآلي:** وهم الخبراء الذين تكون لهم الدراية التامة بتشغيل جهاز الحاسب الآلي والمعدات المتصلة به واستخدام لوحة المفاتيح في إدخال البيانات وتكون لديهم معلومات عن قواعد كتابة البرامج.

- **المحللون**: المحلل هو الشخص الذي يحلل الخطوات. ويقوم بتجميع بيانات نظام معين وتحليلها إلى وحدات منفصلة واستنتاج العلاقات الوظيفية منها.

- **المبرمجون**: وهم الأشخاص المتخصصون في كتابة أوامر البرامج. ويمكن تقسيمهم إلى مخططو برامج التطبيقات (ويقومون بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقومون بتحويلها إلى برامج دقيقة وموثوقة لتحقيق هذه المواصفات) ومخططوا برامج النظم (ويقومون بإختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية وإدخال أية تعديلات أو إضافات لها).

- **مهندسو الصيانة والاتصالات:** وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الإتصال المتعلقة به.

- **مديرو النظم:** وهم الذين يوكل لهم أعمال الإدارة في النظم المعلوماتية. وتخضع الشهادة كوسيلة اثبات إلى اجتهاد القاضي.

٣-معاينة: يقصد بالمعاينة الانتقال إلى الأماكن التي وقعت فيها الجريمة لإثبات حالة الأماكن والأشخاص وكل ما يفيد في كشف الحقيقية عن الجريمة وعن مرتكبها، وبالتالي يجب الانتقال إلى أماكن وقوع الجريمة فور ارتكابها حتى لا يكون هناك فارق زمني طويل بين وقوع الجريمة وإجراء المعاينة التي تسمح للجاني بتغيير أو إزالة كل أو بعض الآثار المادية للجريمة التي تساعد على إظهار الحقيقة. والمعاينة في مجال كشف الجريمة الالكترونية لا تتمتع بنفس الدرجة من الأهمية التي تلعبها في مجال الجريمة التقليدية ومرد ذلك أن هناك مسرحا للجريمة التقليدية والتي يمكن من خلالها كشف الواقعة عن طريق معاينة الآثار المادية التي تخلفها إرتكاب الجريمة وحجز الأشياء التي لها علاقة بالواقعة الإجرامية بينما لا توجد عادة مسرح في الجريمة الكترونية بإعتبار أن مكان الجريمة هو العالم الافتراضي أو عالم الفضاء الإلكتروني والذي يكون عادة الموقع أو المكتب الذي توجد فيه مكونات الحاسب الآلي المادية والمعنوية، والتي تكون محلا للجريمة أو أدلتها وهي تتمثل في الأجهزة والأنظمة والبرامج.

وحتى تحقق المعاينة الغرض المرجو منها في كشف غموض الجريمة ومعرفة الجاني يجب التقيد بعدة شروط وهي) نائلة :٢٠٠٤، ص.٣٢):

- سرعة الانتقال إلى مكان وقوع الجريمة الإلكترونية.

- السيطرة والتحكم على مكان وقوع الجريمة الإلكترونية: وذلك بمنع أي شخص من مغادرة مكان الواقعة ومنع تواجد أي شخص بداخل مسرح الجريمة حتى لا يؤدي إلى تغيير الآثار والأدلة المستمدة من الواقعة وحماية كل ما له علاقة بالحادث من وسائل وأشياء وأشخاص وقيام الخبراء برفع الآثار بمسرح الجريمة.

- الترتيب في المعاينة: يجب اجراء معاينة مرتبة ومتسلسلة وذلك بتحديد نقاط البدء في المعاينة وعدم الانتقال من مكان لآخر إلا بعد التأكد من معاينته تماما.

- الدقة والعناية الفائقة في معاينة مسرح الجريمة الإلكترونية.

- التحفظ على مسرح الجريمة الإلكترونية بعد المعاينة.

- تدوين المعاينة: وذلك إما كتابيا أو تصويريا.

وبالرجوع الى مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصال يتولى معاينة الجرائم مأمورو الضابطة العدلية المشار إليهم بالعددين3 و 4 من الفصل 10 من م.إ.ج ومأمورو الضابطة العدلية العسكرية المنصوص عليهم بالعدد 3 من الفصل 16 من مجلة المرافعات والعقوبات العسكرية والأعوان المحلفون للوزارة المكلفة لتكنولوجيا المعلومات والاتصال المؤهلين للغرض المنصوص عليهم بمجلة الاتصالات.

4-التفتيش: يقصد بالتفتيش الدخول إلى نظم المعالجة الآلية للمعطيات بما تحتويه من مدخلات وتخزين ومخرجات وذلك من أجل البحث عن الأفعال والسلوكات المرتكبة وغير المشروعة والتي تشكل جريمة. ويتم القيام به من طرف وكيل الجمهورية أو قاضي التحقيق أو مأموري الضابطة العدلية المأذونين في ذلك.

وقد يرد محل التفتيش على أنظمة الحاسب الآلي وشبكات الحاسب الآلي.

- تفتيش أنظمة الحاسب الآلي: والتي تشمل المكونات المادية والمعنوية.

تشمل مكونات الحاسوب المادية على الأشياء الملموسة وملحقاته والتي تتمثل في شكل وحدات كوحدة الذاكرة ولوحة المفاتيح ووحدة التحكم. وكل واحدة لها مهمة محددة. وهي لا تواجه صعوبات تعيق إجراءات التفتيش بإعتبارها من المكونات المادية والتي يمكن العثور عليها في مسكن المتهم أو في مكان عام أو غيره من الأماكن. والتفتيش في هذه الحالة يجب أن يتم وفقا للقواعد القانونية التي تحكم التفتيش ...

وتتمثل المكونات المعنوية لجهاز الحاسب الآلي في مجموع البرامج والأساليب المتعلقة بتشغيل وحدة معالجة البيانات. وتنقسم إلى كيانات أساسية تظم البرامج الضرورية التي تقوم بتشغيل واستخدام جهاز الحاسب الآلي وكيانات تطبيقية تضم برامج تمكن المستخدم من أن ينفذ بواسطته عملا معينا.

- شبكات الحاسب الآلي: تخضع شبكات الحاسب الآلي للتفتيش، حيث يجوز القيام بإجراءات التفتيش في منظومة معلوماتية.

والملاحظ أنه يمكن أن يكون حاسب المتهم متصل بغيره من الحواسيب عبر الشبكة الإلكترونية. وهنا يجب التمييز بين ما إذا كان حاسوب المتهم متصلا بآخر داخل إقليم الدولة أو كان متصلا بحاسوب يقع في نطاق إقليم دولة أخرى.

- حالة وجود جهاز متصل بجهاز المتهم داخل الدولة: يمكن تفتيش سجلات البيانات المتصلة في النهاية الطرفية للحاسوب في منزل المتهم مع جهاز أو نهاية طرفية في مكان آخر. حيث يمكن توسيع الحق في تفتيش المساكن إلى نظم المعلومات الموجودة في موقع آخر حينما يهدف إلى إظهار الحقيقة.

- حالة وجود جهاز متصل بجهاز المتهم خارج الدولة: حيث يقوم مرتكبي الجرائم الإلكترونية بتخزين بياناتهم في أنظمة معلوماتية خارج إقليم الدولة بهدف عرقلة جمع الأدلة. ولحل هذا الإشكال يرى جانب من الفقه أن تفتيش أنظمة الحاسب الآلي العابر للحدود لابد أن يتم في إطار إتفاقيات تعاون ثنائية أو دولية.

5- الحج: يقصد بالحجز وضع اليد على شيء مرتبط بجريمة تمت ويفيد في كشف الحقيقة عنها وعن مرتكبها. ويمكن حجز المكونات المادية للحاسب الآلي وملحقاته الذي يشتمل على الحاسوب ومكوناته الأساسية والثانوية. ومن المكونات المادية التي يمكن حجزها: وحدة المعالجة المركزية ولوحة المفاتيح والشاشة والفأرة والأقراص والأشرطة المغناطيسية ولوحة الدوائر الإلكترونية وأجهزة الاتصال عبر شبكة الأنترنت كأجهزة المودام.

وليس من الضروري حجز كل المنظومة حيث يتم نسخ المعطيات محل البحث وكذلك المعطيات اللازمة لفهمها على دعامة تخزين إلكترونية تكون قابلة للحجز.

6-الاختبار: تكمن أهمية الاستعانة بالخبير في أنه ينير الطريق للقاضي لتحقيق العدالة والوصول للحقيقة.

والخبير هو شخص متخصص فنيا في مجال من المجالات الفنية أو العلمية أو غيرها من المجالات الأخرى، ويستطيع من خلال ما لديه من معلومات وخبرة إبداء الرأي في أمر من الأمور المتعلقة بالقضية التي تحتاج إلى خبرة فنية خاصة.

وإذا كانت الاستعانة بخبير فني في المسائل الفنية البحتة في الجرائم التقليدية أمر ضروري فالاستعانة به في مجال الجريمة المعلوماتية أكثر من الضروري وذلك بسبب أن عملية استخلاص الأدلة الجنائية الرقمية تتطلب مهارة ودراية كبيرة في مجال الحاسب الآلي. وينبغي على الخبير أن يكون ملما بالجوانب الفنية والتقنية ومنها:

المعرفة بتركيب الحاسب وصناعته وطرازه ونوع نظام تشغيله الرئيسية والفرعية والأجهزة الطرفية الملحقة به وكلمات المرور وأكواد التشفير.

- ✓ طبيعة البيئة التي يعمل في ظلها الحاسب من حيث تنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية وتحديد أماكن التخزين والوسائل المستخدمة لذلك.
- ✓ المواضيع الرقمية المحتمل تواجد فيها أدلة الإثبات والصور والأشكال التي تتخذها.
- ✓ الكيفية التي يمكن بواسطتها عزل النظام المعلوماتي دون إتلاف أو تغيير أو إفساد الأجهزة.
- ✓ الكيفية التي يتم بواسطتها نقل الأدلة إلى الأوعية دون أن يترتب عن ذلك إتلافها.
- ✓ التمكن من تحويل أدلة الإثبات غير المرئية إلى أدلة مقروءة والمحافظة على الأدلة المستخرجة بشكل يمكن للقاضي أن يفهمها ويستوعبها.
- ✓ وإذا كانت الوسائل التقليدية قد تكفي لإثبات الجرائم التقليدية إلا أنها قد تعجز عن إثبات الجرائم التي ترتكب بالوسائل الإلكترونية. وقد ظهرت وسائل إثبات حديثة تساعد في إثبات الجرائم الإلكترونية.

وسائل الإثبات الحديثة للجرائم الإلكترونية:

ظهرت وسائل إثبات حديثة سهلت الكشف عن الجريمة وتتمثل في وسائل مادية ووسائل إجرائية كما يلى (عباس: ٢٠١٥: ص.١-٢٥٤):

1-الوسائل **المادية الحديثة**: يقصد بالوسائل المادية تلك الأدوات الفنية التي تستخدم في نظم المعلومات والتي تثبت وقوع الجريمة وتحدد الجاني. فالوسائل المادية عبارة عن أدوات او برامج ذات طبيعة تقنية يتم استخدامها بغرض إثبات وقوع الجريمة وتحديد مرتكبها او بالأحرى وسائل فنية الهدف منها جمع مختلف الأدلة الجنائية الرقمية التي يمكن من خلالها الكشف عن ملابسات الجريمة الإلكترونية. ومن بين هذه الوسائل إستخدام بروتوكول IP/TCP والبروكسي Proxy والمعلومات التي تحتويها ملفات الكوكيز Cookies وبرامج التتبع وكشف الإختراق.

- استخدام بروتوكول IP/TCP: يعتبر بروتوكول IP/TCP من أكثر البروتوكولات المستخدمة في شبكة الانترنت لأنه يعتبر جزء أساسي منه، والمسؤول عن تراسل حزم البيانات عبره وتوجهها إلى أهدافها، فهو يوجد بكل جهاز مرتبط بالإنترنت. ويتكون من أربعة أجزاء، فيشير الجزء الأول من اليسار إلى المنطقة الجغرافية، والجزء الثاني لمزود الخدمة، والثالث لمجموعة الحاسبات الآلية المترابطة، وإما الجزء الرابع يحدد الحاسب الآلي الذي تم الاتصال منه.

ويقوم بروتوكول IP بعنونة كل حزمة مع إضافة معلومات أخرى إليها، فيتم استخدام عنوان IP من خلال البحث عن رقم الجهاز وتحديد موقعه الجغرافي، بالإضافة إني إمكانية مراقبة المستخدم من طرف مزود خدمة الإنترنت وتقديم المعلومات التي تفيد في التحقيق بناء على أن لكل جهاز حاسب آلي يتصل بالإنترنت عنوان IP خاص به. و زيادة على ذلك يعمل عنوان IP بشكل متزامن مع بروتوكول آخر وهو بروتوكول التحكم بالنقل TCP والذي تكمن وظيفته في تقسيم المعلومات إلى حزم معلوماتية.وبالرغم من المعلومات المهمة التي يحتويها بروتوكول IP/TCP ، إلا أنه تثار العديد من الصعوبات في استخدامه، إذ أنه يحتوي على معلومات عن جهاز الحاسب الآلي وليس الأشخاص، لذلك فمن الصعوبة إثبات أن شخصا قد ارتكب جريمة معلوماتية، ومع ذلك يمكن أن يستخدم كقرينة ضد مالك أو صاحب هذا الجهاز إلى أن يثبت العكس، ومن جهة أخرى إمكانية استعمال عناوين مزيفة وذلك بوضع معلومات غير صحيحة من أجل تجنب التعرف إليهم، أو حتى استخدام برامج معينة تؤمن لهم سرية تحركاتهم عبر الشبكة، وذلك بإخفاء عنوان IP عن المواقع التي يزورونها.

- **استخدام معلومات الكوكيز** Cookies: عند زيارة مستخدم الإنترنت أي موقع من مواقع الويب، تفتح هذه الأخيرة ملفا صغيرا على القرص الصلب يسمى كوكيز Cookies بهدف جمع بعض المعلومات عنه وتحسين عملية تصفح الموقع، فهو يسجل العديد من المعلومات التي يمكن أن تساعد في التحقيق من بينها تاريخ زيارة الموقع الإلكتروني، أو تاريخ إجراء التعديلات عليه أو الانتهاء منها، وزيادة على ذلك الاحتفاظ بكلمات السر الخاصة بالمستخدم عند زيارته للموقع

استخدام معلومات البروكسي Proxy: لقد تم تطوير تقنية البروكسي Proxy لاستخدامها كحواجز نارية Firewalls لشبكة الإنترنت. والحاجز الناري عبارة عن نظام أمني يفرض توليد جميع الرزم المرسلة أو الواردة من خلال جهاز وحيد، وتمريرها من خلال الحاجز الناري، فالدور الأساسي الذي تقوم به هو قيامها بدور الوسيط بين مستخدم شبكة الإنترنت وبين مواقعها، وذلك بطلب المعلومات من تلك المواقع وتقديمها للمستخدم.

ومن بين أهم ما تتميز به مزودات البروكسي Proxy هو قدرتها في تسريع الوصول إلى شبكة الإنترنت، بالإضافة إلى احتوائها على تدابير أمنية للتحكم بعملية الاتصال بالإنترنت، و مثال ذلك التعرف على الأشخاص المسموح لهم بالاتصال بالشبكة، وتحديد الخدمات التي يمكن استخدامها، أو حتى تحديد الأيام والأوقات المسموح بها بزيارة شبكة الإنترنت. وعليه فكل هذه العمليات والمعلومات التي يحتويها البروكسي Proxy، يتم حفظها في قاعدة بياناته، مما يجعل دورها قوي في الإثبات عن طريق فحص تلك العمليات المحفوظة بها والتي تخص المتهم والموجودة عند مزود الخدمة. وبالرغم من المميزات التى تتمتع بها مزودات البروكسي Proxy إلا أنها تحتوي على عدة مساوئ قد تشكل عائقا في التحقيق، من بينها منع الوصول إلى صفحات المواقع إلكترونية معينة، أو الحصول على صفحات قديمة أو ناقصة أحيانا إلا أن هذا كله لا يمنعها كونها وسيلة هامة ومفيدة في التحقيق.

- استخدام برامج التتبع وكشف الاختراق: إن طبيعة عمل هذه البرامج تكمن في التعرف على محاولات الاختراق، وكشف كافة المعلومات المتعلقة بمن قام بها، وأيضا إشعار الجهة المتضررة من هذه العملية. ومن بين هذه البرامج، برنامج Hack Tracer V1.2، فعندما يرصد أي محاولة للقرصنة أو اختراق جهاز الحاسب الآلي يسارع بإغلاق منافذ الدخول أمام المخترق، ثم يبدأ في عملية اقتفاء أثره حتى يصل إلى الجهاز الذي حدثت العملية من خلاله. ويستعرض هذا البرنامج مجموعة شاملة من بيانات المخترق من حيث عنوان IP الخاص به، وتاريخ حدوث الاختراق باليوم والساعة، وفي الأخير المعلومات الخاصة بمزود الخدمة.

2-**الوسائل الإجرائية الحديثة**: يقصد بالوسائل الإجرائية الحديثة المستخدمة في جمع الأدلة الجنائية الرقمية الإجراءات التي تستعمل أثناء تنفيذ طرق التحقيق الثابتة والمحددة والأساليب المتغيرة وغير المحددة التي تثبت وقوع الجريمة وتحدد شخصية مرتكبها، فالوسائل الإجرائية عبارة عن أساليب محددة قانونا تهدف إلى إثبات وقوع الجريمة وتحدد شخصية مرتكبها، وذلك باستخدام تقنيات وبرامج إلكترونية مختلفة.

وتتمثل هذه الوسائل الإجرائية في اعتراض الاتصالات والمراقبة الالكترونية.

- اعتراض الاتصالات: تعتبر عملية إعتراض محتوى الاتصالات من بين أهم الإجراءات المستحدثة لما لها من أهمية وفائدة في جمع الأدلة الجنائية الرقمية.

وعملية اعتراض الاتصالات يقصد بها اعتراض أو تسجيل أو نسخ الاتصالات التي تتم عن طريق قنوات أو وسائل الاتصال السلكية واللاسلكية، وهذه الاتصالات هي عبارة عن بيانات قابلة للإنتاج والتوزيع والتخزين والاستقبال والعرض.

وينص مشروع القانون المتعلق بمكافحة جرائم أنظمة المعلومات والاتصالات على ان قاضي التحقيق ياذن بالاعتراض الفوري لمحتوى الاتصالات وتسجيلها أو نسخها، ولا يمكن أن تتجاوز مدة الاعتراض ثلاثة أشهر بداية من تاريخ الشروع الفعلي في إنجازه قابلة للتمديد مرة واحدة وبمقتضى قرار معلل من قاضي التحقيق المتعهد بالقضية.

والاعتراض على الاتصالات عادة ما ينصب على رسائل البريد الإلكتروني E-mail، التي تحتوي على العديد من المعلومات كتاريخ إنشاء الرسالة وتاريخ إرسالها أو تلقيها، وكذلك عنوان المرسل، وعنوان المرسل إليه، ولكن تبقى المعلومات التي تحتويها حاشية رسالة البريد الإلكتروني E-mail Header هي الأهم، حيث تتضمن على عنوان IP لمرسل

الرسالة، وطبقا لما تم دراسته من قبل، فعنوان IP يحتوي على معلومات تتمثل في الكمبيوتر الذي تم إرسال منه الرسالة، وأيضا الموقع الجغرافي الذي أرسلت منه، و معلومات عن مزود الخدمة الذي يتعامل معه مرسل الرسالة.

- **المراقبة الالكترونية**: تعرف المراقبة الالكترونية بأنها عمل أمني أساسي له نظام معلومات إلكتروني، يقوم فيه المراقب بمراقبة المراقب بواسطة الأجهزة الالكترونية وعبر شبكة الانترنت، لتحقيق غرض محدد وإفراغ النتيجة في ملف إلكتروني، وتحرير تقارير بالنتيجة.

وينص المشروع المتعلق بمكافحة جرائم أنظمة المعلومات والاتصال على انه لوكيل الجمهورية أو قاضي التحقيق أو مأموري الضابطة العدلية المأذونين في ذلك الإذن بالجمع أو التسجيل الفوري لبيانات حركة إتصالات باستعمال الوسائل الفنية المناسبة والاستعانة في ذلك عند الاقتضاء بمزودي الخدمات كل حسب نوع الخدمة التي يسديها. ويعترض إثبات الجرائم الالكترونية عد ة صعوبات ومنها (أحمد :٢٠٠٢، ص.٦٦):

معوقات إثبات الجريمة الالكترونية:

على الرغم من الجهود المبذولة في إثبات الجريمة الإلكترونية، إلا أن هناك بعض المعوقات في إثباتها. وهي تتمثل في معوقات متعلقة بالدليل ذاته ومعوقات ترتبط بفقدان الآثار المتعلقة بالجريمة ومعوقات ترتبط بتعذر الحصول على الأدلة بالحماية الفنية ومعوقات متعلقة بصعوبة الإبلاغ ونقص خبرة سلطات البحث والتحقيق في الجريمة الالكترونية ومعوقات متعلقة بصعوبة التعاون الدولي وضخامة البيانات المتعلقة بمكافحة الجريمة الالكترونية عن طريق الحاسب الآلي.

معوقات متعلقة بالدليل ذاته يكون دليل الإثبات في الجريمة التقليدية مرئيا من ذلك السلاح الناري أو الأداة الحادة المستعملة في القتل أو الاعتداء بالعنف، أو الكتب الذي تم تزويره، أو النقود التي زيفت وأدوات تزييفها. وفي كل هذه الأمثلة يستطيع مأمور الضابطة العدلية رؤية الدليل المادي وملامسته بإحدى حواسه، ولكن في الجريمة الإلكترونية عن طريق الحاسب الآلي، فإن الوسيلة المستخدمة عبارة عن نبضات إلكترونية غير مرئية تتم عبر أجزاء الحاسب الآلي والشبكة، ولا يقف الأمر عند حد عدم الرؤية، لكنها غالبا مشفرة بحيث لا يمكن للإنسان قراءتها، بل تقرأها الآلة وتظهر على شاشة الحاسب الآلي، ولذلك يمكن للمجرم أن يطمس دليل جريمته طمسا كاملا ولا يترك وراءه أي أثر، ومن ثم يتعذر إن لم يكن مستحيلا ملاحقته أو كشف شخصيته.

ويعد التسلل الإلكتروني من أبرز أمثلة السلوك الإجرامي في الجرائم الإلكترونية، التي يتعذر فيه رؤية دليل الجريمة، حيث يقع استخدام أساليب عالية التقنية في الدخول إلى المناطق المؤمنة والمحمية إلكترونيا أو الوصول إلى مركز الحاسب الآلي للدخول إلى قواعد المعلومات. فالدخول أو التسلل الإلكتروني، يتم عن طريق قيام الجاني بتوصيل جهاز إلى جهاز آخر له حق الدخول وذلك عن طريق خط هاتفي، وعندما يفتح الجهاز المتصل بمركز المعلومات والمسموح له بذلك، نجد أن جهاز الجاني يمارس نشاطه ويحصل على ذات المعلومات دون أن يراه أحد إلى أن يغلق الجهاز الأصلي صاحب الحق في الدخول.

معوقات ترتبط بفقدان الآثار المتعلقة بالجريمة (محمد:٢٠٠٥، ص.٢٣):

تظل الجريمة الإلكترونية عن طريق الحاسب الآلي مجهولة ما لم يبلغ عنها للجهات الخاصة بالبحث أو التحقيق الجنائي. والمشكلة التي تواجه أجهزة العدالة الجنائية أن هذه الجرائم لا تصل لعلم السلطات المعنية بطريقة اعتيادية كباقي جرائم قانون العقوبات، فهي جرائم غير تقليدية، لا تخلف آثار مادية كتلك التي تخلفها الجريمة العادية مثل جثة المجني عليه في القتل، واختلاس المال من المجني عليه في السرقة.

وقد يرجع السبب في افتقاد الآثار التقليدية للجريمة الإلكترونية عن طريق الحاسب الآلي أن هناك بعض العمليات التي يجري إدخال بياناتها مباشرة في جهاز الحاسب الآلي دون أن يتوقف ذلك على وجود وثائق أو مستندات يتم النقل منها، كما لو كان البرنامج معدا ومخزنا على جهاز الحاسب، ويتوافر أمام المتعامل عدة اختيارات، وليس له سوى أن ينقر أو يضغط على الخيار الذي يريد فتكتمل حلقة الأمر المطلوب تنفيذه، كما في المعاملات المالية في البنوك، أو برامج المخازن في الشركات والمؤسسات التجارية الكبرى، حيث يتم ترصيد الأشياء المخزنة أو حسابات العملاء، أو نقلها من مكان لآخر بطبقة آلية وحسب الأوامر المعطاة لجهاز الحاسب الآلي. ويمكن ارتكاب بعض من أنواع الجرائم الإلكترونية كالاختلاس أو التزوير، وذلك بإدخال بيانات غير مطلوبة وغير معتمدة في نظام الحاسب أو تعديل البرنامج المخزن في جهاز الكمبيوتر، وتكون النتيجة مخرجات على حسب متطلبات مستخدم الجهاز الذي أدخل البيانات أو عدل البرامج دون استخدام وثائق أو مستندات ورقية، وبالتالي تفقد الجريمة آثارها التقليدية.

معوقات ترتبط بتعذر الحصول على الأدلة بالحماية الفنية:

إن الهيئات والجهات التي تتبنى في نشاطها نظاما معلوماتيا لتسيير حركتها سواء كانت جهات خدمية أو أمنية أو مؤسسات اقتصادية تحاول دائما الحفاظ على معلوماتها وبياناتها عن طريق تخزين هذه البيانات والمعلومات بعيدا عن أيدي محترفي الجريمة الإلكترونية عن طريق الحاسب الآلي، ويظهر ذلك واضحا في مجال التجارة الإلكترونية، ومنها التعاقد بواسطة الإنترنت. ولذلك تحاول الجهات المعنية بالتجارة الإلكترونية المحافظة على عمليات الدفع الإلكتروني فضلا عن تواصل المعلومات والبيانات بينها وبين الأطراف الأخرى، وكذلك حماية عملية التحويلات المالية، ويتبع في ذلك طريقتين هما استخدام أسلوب التشفير والتحقيق عن شخصية المتعاقدين. وفيما يتعلق بالتشفير فالشفرة متفق عليها بين الطرفين، ويعرف كلاهما مفتاح هذه الشفرة لضمان عدم قراءة الرسالة إلا لمن هو مصرح له بذلك. أما التحقيق عن شخصية المتعاقدين فيتم عن طريق استخدام "شفرة المفتاح العام" حيث يمكن للطرفين المتعاقدين أن يوقعا على المستندات بطريقة رقمية، ويتأكد كل طرف من توقيع الطرف الآخر باستخدام المفتاح العام للشفرة.

وعلى الرغم من قيام الجهات ذات الأنظمة المعلوماتية بحماية نظمها عن طريق الترميز والتشفير وغيرها من طرق الحماية الإلكترونية، فإنه يمكن اختراق هذه الأنظمة، وذلك بالدخول إلى المعلومات السرية أو الأسرار التجارية بغرض بيعها أو استخدامها في مؤسسات جديدة يسعى الجناة إلى إنشائها أو يكون هدفهم فقط تغيير الأرقام والبيانات أي تخريب المعلومات، كما أن الأمور لا تقف عند هذا الحد، بل إن هؤلاء يقومون بفرض تدابير أمنية لمنع التفتيش المتوقع بحثا عن أدلة إدانة ضدهم، وذلك باستخدام كلمات سر حول مواقعهم تمنع الوصول إليها أو ترميزها أو تشفيرها لإعاقة الإطلاع على أي دليل يخلفه نشاطهم الإجرامي، الأمر الذي يعوق الرقابة على البيانات المخزنة أو المنقولة عبر حدود

الدولة. وعمليات الاختراق أو القرصنة الإلكترونية ليست قاصرة داخل المؤسسة أو داخل الدولة بل قد يكون المتدخل من خارج حدود الدولة، ذلك أن التكنولوجيا وثورة الاتصال قد ألغت ما يسمى بالحدود الجغرافية وأصبحت عملية الاختراق الالكتروني تتجه لخدمة المصالح الاقتصادية بين الدول. وذلك يتطلب ضرورة تفعيل التعاون الدولي في مجال مكافحة جريمة الاعتداء على الأموال عن طريق الحاسب الآلي.

معوقات متعلقة بصعوبة الإبلاغ ونقص خبرة سلطات البحث والتحقيق في الجريمة الالكترونية: وتتمثل في (أحمد :٢٠٠٢، ص.٦٦):

1-عدم الرغبة في الإبلاغ عن الجريمة الالكترونية عن طريق الحاسب الآلي: الجريمة في صورتها التقليدية تصل إلى علم سلطات البحث عن طريق الشكوى أو الإبلاغ والتي يجب على الباحث قبولها متى وردت في شأنها جريمة ويحرر بها محضرا يرسله فورا إلى المحكمة. ولكن تظل الجريمة الإلكترونية مستترة ما لم يتم الإبلاغ عنها، فالصعوبة التي تواجهه أجهزة الأمن والمحققين هي أن هذه الجرائم لا تصل إلى علم السلطات المعنية بالصورة العادية وذلك لصعوبة اكتشافها من قبل الأشخاص العاديين أو حتى الشركات والمؤسسات التي وقعت عليها في هذه الجرائم.

ومن أجل تفعيل عملية الإبلاغ عن الجريمة الإلكترونية عن طريق الحاسب الآلي، ومن ثم المساهمة بطريقة إيجابية في منع وقوع الجريمة أو سرعة تحصيل الدليل المتعلق بها، طالب البعض في الولايات المتحدة الأمريكية بأن تتضمن القوانين المتعلقة بالجريمة الإلكترونية، نصوصا تلزم موظفي الجهة المجني عليها - أيا كانت - بضرورة الإبلاغ عما يصل إلى علمهم من جرائم تتعلق بهذا المجال.. إلا أنه ولدى عرض هذا الاقتراح على "لجنة خبراء مجلس أوروبا" قوبل بالرفض لسبب قانوني وهو أن المجني عليه وهو الشركة التي أرتكب في حقها جريمة الاعتداء الإلكتروني، سوف تصبح متهمة بعد أن كانت مجنيا عليها ولذلك وردت اقتراحات بديلة قد تكون مقبولة منها الالتزام بإبلاغ جهة خاصة، أو إبلاغ سلطات إشرافية، وتشكيل أجهزة خاصة لتبادل المعلومات.

ولذلك فإن الشرطة الدولية (الأنتربول) بدأت تهتم بمكافحة جرائم الكومبيوتر وأنشأت لديها فرقة خاصة لهذا الغرض.

2- نقص خبرة سلطات البحث والتحقيق في الجريمة الإلكترونية: من الصعوبات التي تواجه عملية استخلاص الدليل في الجريمة الإلكترونية كذلك نقص الخبرة لدى الباحث، وكذلك لدى أجهزة العدالة الجنائية ممثلة في سلطات الاتهام والتحقيق الجنائي، وذلك فيما يتعلق بثقافة الحاسب الآلي والإلمام بعناصر الجريمة الإلكترونية عن طريق الحاسب الآلي وكيفية التعامل معها، وذلك على الأقل في البلدان العربية. نظرا لأن تجربة الاعتماد على الحاسب الآلي وتقنياته وانتشاره في هذه البلدان جاء متأخرا عن أوروبا وكندا والولايات المتحدة. والي حد الآن فإن الحركة التشريعية والثقافية الأمنية أو القانونية بخصوص هذه الجرائم لا تسير بذات المعدل.

وهذا الفارق في التقدم أو التطور ينعكس سلبا على فنية إجراء الأبحاث والتحقيقات في الجريمة الإلكترونية عن طرق الحاسب الآلي، ومن هنا تأتي الدعوة إلى وجوب تأهيل المختصين في جهات التحقيق والإدعاء تأهيلا مناسبا في شأن هذه الجرائم.

معوقات متعلقة بصعوبة التعاون الدولي وضخامة البيانات المتعلقة بمكافحة الجريمة الإلكترونية عن طريق الحاسب الآلي:

وهي تتمثل في (أحمد :٢٠٠٢، ص.٦٦):

1- صعوبات التعاون الدولي في مكافحة الجريمة الإلكترونية: لقد كان لتقدم شبكة المعلومات الدولية (الإنترنت) مجموعة متنوعة من الاستخدامات في مجال السياحة والإعلام والثقافة والشؤون العسكرية والاقتصادية والأمنية. ولذلك نادى البعض بضرورة إنشاء وحدات خاصة بمكافحة الجريمة الإلكترونية بواسطة الحاسب الآلي والإنترنت أسوة بجهات البحث الجنائي الدولية -الإنتربول -لإثبات الجريمة عند وقوعها وتحديد أدلتها وفاعليها، وهو ما يعنى كذلك إيجاد صيغة ملائمة للتعاون الدولي لمكافحة الجرائم الإلكترونية عن طرق الإنترنت، وتبادل الخبرات والمعلومات حول هذا النوع من الجرائم ومرتكبيها وسبل مكافحتها. ورغم المناداة بضرورة التعاون الدولي في مكافحة الجريمة الإلكترونية عن طريق الحاسب الآلي، إلا أن هناك عوائق تحول دون ذلك، وتجعل هذا التعاون صعباً ومن ذلك: (أحمد :٢٠٠٢، ص.٦٦):

- ✓ عدم وجود نموذج واحد متفق عليه فيما يتعلق بالنشاط الإجرامي: ذلك أن الأنظمة القانونية في بلدان العالم لم تتفق على صور محددة يندرج في إطارها ما يسمى بإساءة استخدام نظم المعلومات الواجب إتباعها، وكذلك ليس هناك تعريف محدد للنشاط المفروض أن يتفق على تجريمه، وذلك نتاج طبيعي لقصور التشريع ذاته في كافة بلدان العالم وعدم مسايرته لسرعة التقدم المعلوماتي.
- ✓ عدم وجود تنسيق فيما يتعلق بالإجراءات الجنائية المتبعة في شأن الجريمة الالكترونية بين الدول المختلفة: خاصة ما تعلق منها بأعمال الاستدلال أو التحقيق، خاصة وأن عملية الحصول على دليل في مثل هذه الجرائم خارج نطاق حدود الدولة، عن طريق لحجز أو التفتيش في نظام معلوماتي معين وهو أمر غاية في الصعوبة، فضلا عن الصعوبة الفنية في الحصول على الدليل ذاته.
- ✓ عدم وجود معاهدات ثنائية أو جماعية بين الدول على نحو يسمح بالتعاون المثمر في مجال هذه الجرائم: وحتى في حال وجودها فإن هذه المعاهدات قاصرة عن تحقيق الحماية المطلوبة في ظل التقدم السريع لنظم برامج الحاسب وشبكة الإنترنت، ومن ثم يظهر الأثر السلبي في التعاون الدولي.
- ✓ مشكلة الاختصاص في الجريمة الإلكترونية: وهي من المشكلات التي تعرقل الحصول على الدليل في الجريمة الإلكترونية عن طرق الحاسب الآلي، ذلك أن هذه الجرائم من أكثر الجرائم التي تثير مسألة الاختصاص على المستوى المحلي والدولي بسبب التداخل والترابط بين شبكات المعلومات، فقد تقع جريمة الحاسب الآلي في مكان معين، ومن هنا تنشأ مشكلة البحث عن الأدلة الجنائية على شبكة الإنترنت، وهذا ما يتطلب خضوع إجراءات التحقيق للقوانين الجنائية السارية في تلك الدول.

2-الصعوبات المتعلقة بضخامة البيانات المتعلقة بالجريمة: لعل من الصعوبات الكبيرة التي تواجه سلطات البحث وسلطات التحقيق الجنائي في الجرائم الإلكترونية عن طريق الحاسب الآلي كمية المعلومات والبيانات الضخمة والتي هي في حاجة إلى فحص ودراسة كي يستخلص منها دليل هده الجريمة، ففضلا عن ضرورة توافر الخبرة الفنية في مجال

الحاسب الآلي والمعلوماتية لدى الباحث أو المحقق، يتعين كذلك أن يتوافر لديه القدرة على فحص هذا الكم الهائل من المعلومات والبيانات المخزنة على الحاسب الآلي أو على ديسكات أو اسطوانات منفصلة.

ولذلك يمكن القول أن ضخامة هده البيانات والمعلومات، تعد عائقا في تحقيق الجرائم الإلكترونية عن طريق الحاسب الآلي، ذلك أن طباعة كل ما هو موجود على الدعامات المغنطة لحاسب متوسط العمر، يتطلب مئات الآلاف من الصفحات، في الوقت الذي قد لا تقدم فيه هذه الصفحات شيئا مفيدا للتحقيق وهذا عكس ضخامة أو وفرة المعلومات في الجرائم التقليدية كالقتل أو السرقة، ذلك أن وفرة المعلومات في مثل هذه الجرائم هو أمر يساعد العدالة ويساعد الباحث أو المحقق-على السواء -في استخلاص الدليل الجنائي في هذه الجريمة. (أحمد :٢٠٠٢، ص.٦٦).

٤-دور مختلف المؤسسات في مكافحة الجريمة الالكترونية:

١/٤ المحاكم والقضاء:

المحكمة الدستورية العليا ومبدأ الشرعية الجنائية للجريمة الالكترونية: تلعب المحكمة الدستورية العليا دور كبير في إرساء دعائم مبدأ شرعية الجرائم والعقوبات باعتبارها أحد تطبيقات فكرة الأمن القانوني، فعملت علي استجلاء حقيقته وفحواه ودلالته وماهيته ومداه والضوابط التي تقيده، ووضعت الضوابط الصحيحة لتفويض السلطة التنفيذية في بعض جوانب التجريم والعقاب، واستخلصت فكرة عدم جواز توقيع عقوبة إلا بناء على حكم قضائي، ومفهوم الجريمة من الناحية القانونية، ووضعت الضوابط التي بموجبها تباشر رقابتها على دستورية النص الجنائي(على :٢٠١٠، ص.١٥).

أكدت المحكمة الدستورية العليا علي أهمية مبدأ الشرعية الجنائية فقضت بأن" استقرار مبدأ شرعية الجرائم والعقوبات في مفاهيم الدول المتحضرة، دعا إلى توكيده ، ومن ثم وجد صداه في عديد المواثيق الدولية من بينها الفقرة 11 من الإعلان العالمي لحقوق الإنسان، والفقرة الأولي من المادة 15 من العهد الدولى للحقوق المدنية والسياسية، والمادة 7 من الاتفاقية الأوربية لحماية حقوق الإنسان كما تردد في العديد من الدساتير، " فغدا أصلا ثابتا وضمانة ضد التحكم، فلا يؤثم القاضي أفعالاً ينتقيها ولا يقرر عقوباتها وفق اختياره، إشباعا لنزوة أو انفلاتا عن الحق والعدل . وصار التأثيم بالتالي – وبعد زوال السلطة المنفردة، عائدا إلى المشرع؛ إذ يقرر للجرائم التي يحدثها عقوباتها التي يجرمها، ويفسر هذا المبدأ بأن القيم الجوهرية التي يصدر القانون الجنائي لحمايتها، لا يمكن بلورتها إلا من خلال السلطة التشريعية التي انتخبها المواطنون لتمثيلهم، وأن تعبيرها عن إرادتهم يقتضي أن تكون بيد سلطة التقرير في شأن تحديد الأفعال التي لا يجوز تأثيمها وعقوبتها لضمان مشروعيتها. ومن ثم كان المبدأ لازما لتمكين المواطنين من الاتصال بتلك القيم التي يقوم عليها بنيان مجتمعهم، بما يوحد التي يقوم عليها بنيان مجتمعهم، بما يوحد بينهم ويكفل تماسكهم اجتماعيا فلا يزدرونها.

أكدت على ارتباط مبدأ الشرعية الجنائية والسياسية الجنائية للدولة في حكمها؛ لأن" السياسة الجنائية الرشيدة يتعين أن تقوم على عناصر متجانسة، فإن قامت على عناصر متنافرة نجم عن ذلك افتقاد الصلة بين النصوص ومراميها، بحيث لا تكون مؤدية إلى تحقيق الغاية المقصودة منها لانعدام الرابطة المنطقية بينهما، إيمانا بأن الأصل في النصوص التشريعية – في الدولة القانونية-هو ارتباطها عقلا بأهدافها، باعتبار أن أي تنظيم تشريعي ليس

مقصودا لذاته، وإنما هو مجرد وسيلة لتحقيق تلك الأهداف. ومن ثم يتعين دائما استظهار ما إذا كان النص المطعون عليه يلتزم إطار منطقيا للدائرة التي يعمل فيها، كافلا تناغم الأغراض التي يستهدفها أو متناقضا مع مقاصده أو مجاوزا لها مناهضا – بالتالي لمبدأ خضوع الدولة للقانون. أكدت على ارتباط مبدأ الشرعية الجنائية والعدالة الجنائية للدولة في حكمها لأن" العدالة الجنائية في جوهر ملامحها، هي التي يتعين ضمانها من خلال قواعد محددة تحديدا دقيقاً، ومنصفا، يتقرر على صونها ما إذا كان المتهم مدانا أو بريئا، ويفترض ذلك توازنا بين مصلحة الجماعة في استقرار أمنها، ومصلحة المتهم هي ألا تفرض عليه عقوبة ليس لها من صلة بفعل أتاه، أو تفتقر هذه الصلة إلى دليل يؤكدها، ولا يجوز النزول عنها أو التفريط فيها (أحمد :٢٠٠٢، ص.٦٦).

بالنسبة للقضاء: يلتزم بتطبيق النص الجنائي المتعلق بالجريمة الالكترونية دون تعديل بالإضافة أو بالحذف سواء بالنسبة لشق التجريم أو العقاب، فيتعين عليه في البداية أن يحدد ما إذا كانت الواقعة تندرج تحت أحد النماذج الإجرامية التى قررها المشرع أم لا، فإذا لم يثبت ذلك وجب الحكم ببراءة المتهم، أماإذا كانت الواقعة مجرمة وجب عليه أن يضع لها التكييف القانوني السليم(نائلة :٢٠٠٤، ص.٣٢).

٢/٤ النيابة لعامة:

بالنسبة للسلطة التنفيذية والنيابة العامة: تلتزم الجهات القائمة على التنفيذ العقابي بتنفيذ الحكم بذات الأوضاع التي نص عليها القانون، وبالتالي فإن الإدارة لا تستطيع أن تنفذ عقوبة لم يقض بها حكم قضائي أو أن تحل نفسها محل القضاء في تطبيق العقوبة، أو أن تظل تنفذ العقوبة على خلاف مقتضى الحكم القضائي (هدى :٢٠١٠، ص.٤٢).

٣/٤ المخابر الجنائية:

يسهم المختبر الجنائي في كشف غموض الجرائم وتحديد هوية المجرمين بالدليل العلمي والأدلة المادية من خلال إجراء عمليات التحليل والفحص للمواد المتحصلة من مسرح الجريمة، ويلعب المختبر الجنائي دورا مهما في مواجهة الجريمة ومكافحتها، لما يحتويه من كوادر بشرية مؤهلة وتقنيات حديثة لإجراء الفحوصات الكيميائية والفيزيائية والبيولوجية واستخلاص النتائج لتحديد الجناة، ما يؤدي إلى تعزيز الأمن والاستقرار وإشاعة أجواء الطمأنينة وحماية الممتلكات العامة والخاصة. (هدى :٢٠١٠، ص.٤٢).

اعتمدت الكثير من الأجهزة الأمنية بدول العالم في الماضي على إيجاد الحلقة المفقودة في سلسلة الأدلة التي يمكن من خلالها التوصل إلى الحقيقة وكشف أسلوب ارتكاب الجرائم، حيث كان التحقيق مع المتهمين يعتمد على الاعترافات سواء كانت صحيحة أم خاطئة وفي بعض الأحيان يتم اللجوء لوسائل التعذيب للوصول إلى الحقيقة، وبمرور الأيام أصبحت هذه الوسائل غير مجدية وذلك لتعرض بعض الأبرياء للعقاب نظير جريمة لم يقترفوها وكذلك تطور أساليب الإجرام والجريمة، من هنا بدأ التفكير الجدي للبحث عن وسائل أخرى أكثر نفعا لمساعدة رجال الشرطة والقضاة للوصول إلى الحقيقة دون التعرض لسلامة وكرامة المتهمين وسلب حقوقهم المشروعة. (هدى :٢٠١٠، ص.٤٢).

من هذا المنطلق حذت معظم الدول العربية حذو الدول المتقدمة في تطوير وتعزيز قدراتها الأمنية من خلال إنشاء الأجهزة الفنية الخاصة بكشف الأدلة المادية، وهذه الأجهزة تعد بمثابة الرابط المكمل لدور الأجهزة الأمنية وأصبح

مطلباً ملحاً وضرورياً لتحقيق مبدأ العدالة، حيث مرت إدارة الأدلة الجنائية عبر تاريخها بعدد من التغيرات وذلك بسبب تزايد عدد الجرائم وتغير نمط ارتكابها حيث ظهرت الحاجة إلى استحداث أقسام متخصصة في فحص الأدلة المادية المتحصلة من مسارح الجريمة وذلك لدعم الأدلة المعنوية وتقويتها. وحرص الدول في إدخال التقنيات الحديثة والمتطورة في مجال المختبرات الجنائية.

ويضم المخبر الجنائى الإدارة، وفرع السموم والعقاقير الذي يعتبر من الفروع الحيوية المسؤولة عن عمليات فحص وتحليل السموم والعقاقير، المتمثلة في المخدرات والسموم العضوية وغير العضوية والأدوية الشعبية بمختلف أشكالها عن طرق تحليل سوائل الجسم (الإدرار والدم) والأحشاء الداخلية للجسم ويتم ذلك بواسطة الطرق التحليلية وأجهزة التحليل للتعرف على المواد السامة والمخدرات والتحقق من وجودها وتحديد وظيفة كل منها ودرجة خطورتها. كذلك فرع الأحياء والبصمة الوراثية ((DNAالذي يتولى مسؤولية التحليل والتصنيف للعينات الحيوية بالطرق العلمية والأجهزة المتقدمة التي من خلالها يمكن التعرف على فصائل الدم المختلفة وتحديد نوعها والتعرف على الألياف والشعر والنباتات وتحديد نوعها ، كما يقوم بمباشرة القضايا الجنسية كالاغتصاب وغيرها والتحقق من وقوع الجريمة وذلك من خلال الفحوصات التأكيدية في فحص الملابس والمسحات والآثار الأخرى، حيث يواكب المختبر الجنائي التطور الحاصل على مستوى الفحوصات الحيوية ففي عام 1989م أستحدث قسم لفحص البصمة الوراثية DNAوالاستفادة من هذه التقنية الفعالة كدليل مادي قوي من خلال فحص سوائل الجسم في حوادث القتل والاغتصاب وقضايا البنوة والهجرة، كما استطاع المختبر الجنائي حالياً من إنشاء قاعدة بيانات لتصنيف البصمة الوراثية لأصحاب السوابق والمشتبه بهم. كما يضم فرع الفيزياء والكيمياء، الذي يجري العديد من الفحوصات للقضايا المتعلقة بحوادث الحرائق الجنائية والسرقات وحوادث المرور وجرائم القتل وغيرها، وتتلخص تلك الفحوصات في فحص المعادن الثمينة، الزجاج، آثار الأقدام والإطارات، آثار الآلات، الأصباغ، الأحبار وغيرها، وتشير الإحصائيات السنوية للقضايا والفحوصات في المختبر الجنائي إلى أن معدلات حوادث الحريق هي الأكثر شيوعاً، كما يتولى الفرع مهمة فحص الأسلحة النارية والذخيرة في حوادث إطلاق النار أو حيازة الأسلحة والذخيرة وذلك للتعرف عليها وتصنيفها وتحديد نوع السلاح المستخدم في الحوادث من خلال أجهزة الكشف والمقارنة المتوفرة لدى الوحدة والتي عن طريقها يمكن الوصول إلى الحقائق وتنوير العدالة بالطرق والأساليب المتعلقة دولياً. ويقدم المختبر الجنائي المساعدة في الحوادث المرورية المتعلقة بحوادث الاصطدام والهروب وما يتخلف عن تلك الحوادث من أدلة مادية من خلال جمع العينات من مكان الحادث للتعرف على المركبات المتسببة بالحوادث وغيرها. كذلك فرع الأبحاث والكيمياء، فقد أعطى المختبر الجنائي أهمية بالغة للبحث والتطوير، إذ يقوم بدور بارز ومهم في معايرة الطرق التحليلية والأجهزة المعمول بها في المختبر إضافةً إلى إجراء الفحوصات المحالة للفرع والمتعلقة بفحص الأصباغ والألياف والبلاستيك والزيوت والمواد المزيلة للطلاء وكذلك المواد السامة (المعدنية وغير المعدنية)، وأصبح فرع الأبحاث والكيمياء واحداً من الفروع الأكثر أهمية وفاعلية في البحث ودراسة القضايا المتعلقة بالعبوات والمواد المتفجرة والكشف على نوعية المواد المستخدمة فيها علاوةً على فحص المفرقعات والمواد المسيلة للدموع بجانب ما يقدمه الفرع من مساعدة ودعم فني للوحدات الأخرى من خلال إجراء الفحوصات التحليلية للمواد الكيميائية المجهولة (نائلة :٢٠٠٤، ص.٣٢).

وتعد الأدلة الجنائية الرقمية هي فرع من فروع علوم الأدلة الجنائية يتناول البحث عن البيانات المخزنة في أجهزة إلكترونية، والحصول عليها ومعاملتها وتحليلها والإبلاغ بها.وتشكل الأدلة الإلكترونية أحد مكوِّنات جميع الأنشطة الجنائية تقريبا، ومن الأهمية بمكان دعم التحقيقات التي تجريها أجهزة إنفاذ القانون في مجال الأدلة الجنائية الرقمية. ويمكن جمع هذه الأدلة من مصادر متنوعة مثل الحواسيب والهواتف الذكية وأجهزة التخزين عن بُعد والطائرات بدون طيار والمعدات المحمولة على متن السفن وغيرها. والهدف الرئيسي للأدلة الجنائية الرقمية هو استخراج البيانات من الأدلة الإلكترونية، ومعاملتها وتحويلها إلى بيانات استخباراتية يمكن التحرك على أساسها، وتقديم النتائج في سياق الملاحقات القضائية. وتُستخدم في إطار جميع هذه العمليات تقنيات سليمة في مجال الأدلة الجنائية لضمان قبول النتائج في المحكمة(نائلة :٢٠٠٤، ص.٣٢).

النتائج:

توصلت الدراسة للنتائج التالية:

- ✓ التعرف على الإطار المفاهيمى للجريمة الالكترونية.
- ✓ التعرف على الجرائم المتصلة بالجرائم الالكترونية
- ✓ تحديد دور مختلف المؤسسات في مكافحة الجريمة الالكترونية
- ✓ التعرف على موقف الشريعة الاسلامية والقانون الوضعي من الجريمة المعلوماتية
- ✓ التعرف عل الطرق المنوطة بإثبات هاته الجرائم
- ✓ التعرف على كيفية تعامل الجهات المختصة مع الجرائم الالكترونية
- ✓ اقتراح بعض الحلول الممكنة للحد من هاته الجرائم وسبل مكافحتها
- ✓ معرفة مدى مواكبة المشرع العربي للقوانين المعاصرة في مجال المعلوماتية
- ✓ إن الجرائم الالكترونية من الجرائم التى تمس الاقتصاد الوطني والدولي كما أنها تمس منظومة الأخلاق فى المجتمع.
- ✓ الجرائم الالكترونية تأخذ صور متعددة وكل صورة تثير مشكلات موضوعية وإجرائية.
- ✓ هناك حلولا تشريعية وعملية يمكن من خلالها مواجهة تحديات ومشكلات الجرائم الالكترونية.
- ✓ هناك تضارب فى الجهود الوطنية والدولية فى مواجهة تحديات ومشكلات الجرائم الالكترونية، وتلق يؤدى إلى جعل ومكافحة هذه الجرائم هبا منثورا، لأن هناك قلة معرفة وخبرة لمواجهة هذا النوع من الجرائم.

التوصيات:

توصى الدراسة بالأتى:

- ✓ ضرورة تدخل المشرع فى جميع دول العالم لإصدار قانون خاص بالجرائم الالكترونية.
- ✓ ضرورة النظر بمفهوم جديد وليس تقليدى للمال بحيث يشمل المعلومات والبيانات.

✓ ضرورة العمل على تشديد الإجراءات الجنائية للجرائم الإلكترونية بحيث تستوعب التحرى والملاحقة والتحقيق والاستدلال والضبط الالكتروني والتفتيش الالكتروني ووسائله وإجراءات المعاينة والخبرة لان القواعد التقليدية لا تتلاءم وطبيعة الجرائم الالكترونية.

✓ تجريم جرائم أنظمة المعلومات ومنها المتابعة والملاحقة الالكترونية والتشهير وتسوية السمعة والاحتيال الالكتروني.

✓ ضرورة تبنى الدول فكرة إنشاء جهاز خاص بالخبرة الجنائية للجرائم الإلكترونية

✓ ضرورة تدريب أفراد الضابطة العدلية والنيابة العامة والقضاه وتأهيلهم على كيفية التعامل مع الجرائم الالكترونية وآليات جمع الأدلة والتفتيش والتحري والملاحقة والتحقيق والاستدلال.

✓ تطوير القدرات التقنية على شبكة الإنترنت وانشاء جهاز شرطة الإنترنت للقبض المباشر على مرتكبي الجرائم الالكترونية حال دخولهم على الشبكة من خلال التتبع التقنى للجهاز أو الهاتف.

✓ عدم فتح الرسائل الإلكترونية مجهولة المصدر ووضع أرقام سرية على الملفات الهامة.

✓ تضافر الجهود الدولية من أجل سن القوانين والتشريعات الدولية المستمدة من الشريعة الإسلامية لمواجهة الجرائم الالكترونية.

✓ ووضع الضوابط التى تمنع الغزو الثقافى للافكار المنحرفة والمواقع الاباحية.

✓ جعل القرصنة على البرامج بمثابة جرائم سرقة وإنشاء محاكم لقضايا الإنترنت.

✓ توعية الأطفال بعدم ذكر اى معلومات شخصية أو بيانات أو أسماء أو عناوين حقيقة على الشبكة دون إذن الآباء.

قائمة المراجع:

1) إبراهيم المنجى (٢٠٠٢)، عقد نقل التكنولوجيا . التنظيم القانوني لعقد نقل التكنولوجيا والتجارة الإلكترونية .الإسكندرية . منشأة المعارف.

2) إبراهيم حامد طنطاوى، علي محمود حمودة (٢٠١٦)، شرح الأحكام العامة لقانون العقوبات الجزء الأول النظرية العامة للجريمة، دار النهضة العربية، الطبعة الأولى.

3) ابراهيم رمضان ابراهيم عطايا (٢٠١٥)، الجريمة الإلكترونية وسبل مواجهتها فى الشريعة الإسلامية والأنظمة الدولية دراسة تحليلية تطبيقية، مجلة كلية الشريعة والقانون، جامعة طنطا، العدد ٣٠، الجزء الثانى

4) أحمد خليفة (٢٠٠٥)، الجرائم المعلوماتية، الإسكندرية، دار الفكر الجامعي.

5) أحمد حسام طه .(٢٠٠٠)، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، دار النهضة العربية القاهرة، الطبعة الأولى.

6) أحمد فتحى سرور(٢٠٠٢)، القانون الجنائي الدستورى، دار الشروق، الطبعة الثانية.

7) أيمن عبد الحفيظ(٢٠٠٥)، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية، الطبعة الأولى.

8) أيمن عبد الحفيظ(٢٠٠٥)، الاتجاهات الفنية والأمنية لمواجهة الجرائم المعلوماتية.

9) البشرى محمد الأمين(٢٠٠٤)، التحقيق فى الجرائم المستحدثة، جامعة نايف للعلوم الأمنية، الرياض
10) حسنى الجندى (١٩٩٩)، شرح قانون العقوبات، دار النهضة العربية.
11) حسين بن سعيد الغافري(٢٠٠٩)، السياسة الجنائية في مواجهة جرائم الإنترنت دراسة مقارنة، دار النهضة العربية.
12) خالد عبد الله الشافي(٢٠١٠)، المبادىء الجنائية الدستورية في النظام الأساسي للحكم في المملكة العربية السعودية دراسة مقارنة، رسالة دكتوراه، جامعة نايف العربية للعلوم الأمنية، الرياض، المملكة العربية السعودية.
13) خالد ممدوح إبراهيم (٢٠٠١)، حجية البريد الإلكتروني فى الإثبات، ط 1، الإسكندرية، دار الفكر الجامعي.
14) خالد ممدوح إبراهيم(٢٠٠٩)، الجرائم المعلوماتية، دار الفكر الجامعي.
15) ذايب البداينة، جرائم الحاسب والإنترنت، الندوة العلمية لدراسة الظواهر الإجرامية المستحدثة وسبل مواجهتها، أكاديمية نايف العربية للعلوم الأمنية.
16) ذياب موسى البدنية (٢٠١٤)، الجرائم الالكترونية: المفهوم والأسباب، ورقة بحثية قدمت للملتقى العلمى بعنوان الجرائم المستحدثة فى ظل التحولات الإقليمية والدولية خلال الفترة ٢-٢٠٢٢/٩/٤، عمان ،. الاردن.
17) رامى متولي القاضي (٢٠١١)، مكافحة الجرائم المعلوماتية في التشريعات المقارنة وفي ضوء الاتفاقيات والمواثيق الدولية، دار النهضة العربية، الطبعة الأولى.
18) شمسان ناجى صالح ألخيلي (٢٠٠٩)، الجرائم المستخدمة بطرق غير مشروعة لشبكة الإنترنت دراسة مقارنة، دار النهضة العربية.
19) عباس حفصي (٢٠١٥)، جريمة التزوير الالكترونية دراسة مقارنة، رسالة دكتوراه فى العلوم الإسلامية والشرعية، كلية العلوم الإنسانية والعلوم الإسلامية، جامعة وهران ١.أحمد بن بله
20) عبد العظيم مرسي وزير(٢٠١٢)، شرح قانون العقوبات، دار النهضة العربية.
21) عثامنية لخميسي (٢٠٠٥)، التفسير في المادة الجزائية وأثره على حركة التشريع، مجلة العلوم الانسانية، جامعة محمد خضيرة بسكره، العدد السابع، فبراير 2005.
22) على بن هادى البشري (٢٠١٠)، جرائم الحاسب الآلي، الطبعة الأولى، الرياض.
23) عمر سالم(٢٠١٠)، شرح قانون العقوبات المصري، دار النهضة العربية، مصر.
24) محمد سعيد عبد المهدى، أحمد العجلونى (٢٠٠٥)، قواعد تفسير النصوص وتطبيقاتها في الاجتهاد القضائي الأردنى: دراسة أصولية مقارنة، رسالة دكتوراه، كلية الدراسات العليا، الجامعة الأردنية.
25) محمد محمد شتات (٢٠٠١)، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة، الإسكندرية.
26) محمود علي أحمد مدني(٢٠١٥)، دور المحكمة الدستورية العليا في استجلاء المفاهيم الأساسية التى يقوم عليها النظام القانونى المصري "دراسة مقارنة" رسالة دكتوراه، حقوق حلوان.
27) مصطفي محمد موسي (٢٠٠٨)، التحقيق الجنائي في الجرائم الالكترونية، الطبعة الأولى.

28) نائلة عادل محمد فريد قورة(٢٠٠٤)، جرائم الحاسب الاقتصادية" دراسة نظرية وتطبيقية"، دار النهضة العربية.

29) هدى حامد قشقوش(٢٠١٠)، شرح قانون العقوبات، دار النهضة العربية.

30) هلال بن محمد بن حارب البوسعيدى(٢٠٠٩)، الحماية القانونية والفنية لقواعد المعلومات المحوسبة" دراسة قانونية وفنية مقارنة"، دار النهضة العربية.

31) هلال عبد الله أحمد(٢٠٠٢)، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة 23 نوفمبر 2001، دار النهضة العربية.

الجريمة المعلوماتية بين تطور المجتمع الرقمي وحدود التفاعل التشريعي والقضائي

Cybercrime between the development of the digital society and the limits of legislative and judicial interactions

د..صفاء الإدريسي الشرفي/ جامعة محمد الخامس، الرباط/المغرب

Dr.Safae idrissi chorfi/ Mohamed V University, Rabat/ Morocco

ملخص الدراسة:

إن الجرائم بطبيعتها توجد بوجود الإنسان وتتطور بتطوره، وبما أن الإنسان دائما في تطور مستمر بفضل ثورة المعلوميات والتكنولوجيا المتطورة فإننا نجد العلماء والصالحون يحاولون الاستفادة منها، وبالمقابل نجد أن المجرمين يحاولون الاستفادة أيضا من التقدم التقني فأصبحت التكنولوجيا كلأ للجميع الصالح والطالح، بل إن المجرمين كثر، واستطاعوا اكتساب خبرات ومهارات أكثر في تعاملهم مع الانترنيت وارتكابهم للجرائم الإلكترونية، ولم تعد جرائمهم تقتصر على دولة واحدة بعينها بل تجاوزت حدود الدولة.

وكما هو الحال في جميع الدول، لم يبق المغرب بمنأى عن هذا النوع من الإجرام لكنه تأخر إلى حد ما في تضمين تشريعه الجنائي مقتضيات تتصدى لهذا النوع من الجرائم وخاصة جرائم المس بنظم المعالجة الآلية للمعطيات، مما دعا الفقه إلى المطالبة بالإسراع بسن قانون في الموضوع، وفي ظل تزايد وتنامي عدد قضايا المس بنظم المعالجة الألية للمعطيات فإن المغرب لم يستطيع البقاء بمعزل عن التعامل على مستوى التشريع مع ظاهرة المعلوميات فاضطر إلى سن تشريع يتلاءم وخصوصية الجريمة المعلوماتية انسجاما مع مبدأ الشرعية وقد أطلق عليه تسمية "المس بنظم المعالجة الآلية للمعطيات.

وتهدف هذه المداخلة المندرجة ضمن المحور الثاني من محاور المؤتمر: **"مواجهة الجرائم الإلكترونية وطرق إثباتها"** إلى تسليط الضوء على أهم الجرائم المنصوص علها في القانون رقم 03.07 مع تقييمها والوقوف عند الإشكاليات التي تطرحها، مع تناول المقاربة القضائية لمحاربة هذه الجرائم، الأمر الذي يدفعنا إلى الخوض في إشكالية رئيسية تتمثل في **إلى أي حد كان المشرع المغربي موفقا في مواجهة الإجرام المعلوماتي سواء على المستوى الموضوعي أو على المستوى المسطري؟**

الكلمات المفتاحية: الجرائم المعلوماتية، الحاسب الآلي، التكنولوجيا، العولمة

Abstract :

Crimes by their nature exist in the presence of man and develop with his development, and since man is always in continuous development thanks to the revolution of informatics and advanced technology, we find scholars and righteous people trying to benefit from them, and on the other hand, we find that criminals are also trying to benefit from technical progress, so technology has become a food for all, the good and the bad, but the criminals are many And they were able to gain more experience and skills in dealing with the Internet and committing cybercrimes, and their crimes are no longer confined to one particular country, but rather exceed the borders of the state.

As is the case in all countries, Morocco did not remain immune from this type of crime, but it was somewhat late in including in its criminal legislation requirements that address this type of crime, especially crimes against the automated data

processing systems, which prompted jurisprudence to demand the speedy enactment of a law on the matter. In light of the increasing and growing number of cases of damage to automated data processing systems, Morocco could not remain isolated from dealing at the level of legislation with the information phenomenon, so it was forced to enact legislation that is compatible with the specificity of information crime in line with the principle of legitimacy, and it was called "harming automated data processing systems."

This intervention, which falls within the second axis of the conference's themes: "Confronting Cybercrime and Methods of Proving It," aims to shed light on the most important crimes stipulated in Law No. 03.07, evaluate them and stand at the problems they raise, while addressing the judicial approach to combating these crimes, which leads us to To delve into a major problem represented in the extent to which the Moroccan legislator has been successful in confronting information crime, whether at the substantive level or on the underpinning level?

KeyWords : Computer, automated data processing, technology, Globalisatio

مقدمة:

إن الجرائم بطبيعتها توجد بوجود الإنسان وتتطور بتطوره، وبما أن الإنسان دائما في تطور مستمر بفضل ثورة المعلوميات والتكنولوجيا المتطورة (شتا، 2001، صفحة 62) فإننا نجد العلماء والصالحون يحاولون الاستفادة منها، وبالمقابل نجد أن المجرمين يحاولون الاستفادة أيضا من التقدم التقني فأصبحت التكنولوجيا كلأ للجميع الصالح والطالح، بل إن المجرمين كثر، واستطاعوا اكتساب خبرات ومهارات أكثر في تعاملهم مع الانترنيت وارتكابهم للجرائم الإلكترونية، ولم تعد جرائمهم تقتصر على دولة واحدة بعينها بل تجاوزت حدود الدولة.

وكما هو معلوم فقد أدى الحاسب الآلي دورا مهما في انتشار العولمة حيث عمل على التقريب بين الأشخاص وأتاح الفرص للاطلاع على المعلومات، كما مهد الطريق لتبادلها واستغلالها وتخزينها، وفي مقابل هذه الإيجابيات صاحب ذلك مجموعة من الانعكاسات السلبية الخطيرة بسبب سوء استخدام هذه التقنية والانحراف بها عن الأغراض المتوخاة منها، تتمثل أساسا في اعتداءاتها على القيم ومصالح جوهرية تمس الأفراد والمؤسسات، بل وحتى الدول كما تطال حقوق الغير.

وقد تباينت الصور الإجرامية لظاهرة الجرائم الإلكترونية، وتشعبت أنواعها، فمنها ما يتصل بالاعتداء على ذات النظام الإلكتروني، ومنها ما يتعلق بالاعتداء على المعلومات، ومنها أيضا الاحتيال الإلكتروني، والتزوير الإلكتروني، وجرائم الاعتداء على الحق في الخصوصية إضافة إلى جرائم الاعتداء على التحويلات المالية الإلكترونية. (العجمي، 2015)

وكما هو الحال في جميع الدول، لم يبق المغرب بمنأى عن هذا النوع من الإجرام لكنه تأخر إلى حد ما في تضمين تشريعه الجنائي مقتضيات تتصدى لهذا النوع من الجرائم وخاصة جرائم المس بنظم المعالجة الآلية للمعطيات، مما دعا الفقه إلى المطالبة بالإسراع بسن قانون في الموضوع، وفي ظل تزايد وتنامي عدد قضايا المس بنظم

المعالجة الألية للمعطيات فإن المغرب لم يستطيع البقاء بمعزل عن التعامل على مستوى التشريع مع ظاهرة المعلوميات فاضطر إلى سن تشريع يتلاءم وخصوصية الجريمة المعلوماتية (زروق، 2008) انسجاما مع مبدأ الشرعية وقد أطلق عليه تسمية "المس بنظم المعالجة الآلية للمعطيات.

أولا-أهمية النشر العلمي:

لموضوع هذه المداخلة أهمية نظرية وعملية لكونه يمس كثيرا من مصالح المجتمع، كما تظهر أهميته في تحديد مصادر المخاطر التي تهدد النظام الإلكتروني ونظم الشبكات، وتحديد صور الاعتداء على المعلومات والأنماط المستجدة للجرائم الإلكترونية، كما تكمن أهمية هذه المداخلة في محاولة إيجاد الحلول للمشكلات التي تثيرها الجرائم الإلكترونية على مستوى القضاء والقانون.

ثانيا-أهمية التطورات التكنولوجية في مجال النشر العلمي:

تلعب المعلومات دورا هام وحيوي يظهر ذلك في:

- ✓ اثراء البحث العلمي وتطوير العلوم والتكنولوجيا
- ✓ تساهم في بناء استراتيجيات المعلومات على المستوى الوطني
- ✓ لها أهمية كبرى في مجالات التنمية الاقتصادية والاجتماعية والإدارية والثقافية وغيرها
- ✓ تعتبر العنصر الأساسي في صنع واتخاذ القرار المناسب وحل المشكلة
- ✓ تساعد المعلومات في نقل خبراتنا للآخرين وعلى حل المشكلات التي تواجهنا وعلى الاستفادة من المعرفة المتاحة

وتهدف هذه المداخلة المندرجة ضمن المحور الثاني من محاور المؤتمر: "**مواجهة الجرائم الإلكترونية وطرق إثباتها**" إلى تسليط الضوء على أهم الجرائم المنصوص عليها في القانون رقم 03.07 مع تقييمها والوقوف عند الإشكاليات التي تطرحها، مع تناول المقاربة القضائية لمحاربة هذه الجرائم، الأمر الذي يدفعنا إلى الخوض في إشكالية رئيسية تتمثل **في إلى أي حد كان المشرع المغربي موفقا في مواجهة الإجرام المعلوماتي سواء على المستوى الموضوعي أو على المستوى المسطري؟**

ويتفرع عن هذه الإشكالية تساؤلات عدة أهمها:

- ✓ ما مدى استيعاب القضاء المغربي لخصوصية هذا النوع من الإجرام؟
- ✓ ما هي الإمكانات المتاحة أمام المجتمع الدولي والوطني من أجل تجاوز المعيقات القانونية والواقعية التي تواجه التعاون الدولي؟
- ✓ ما مدى مواكبة المشرع المغربي للقوانين المعاصرة في مواجهة الجريمة المعلوماتية؟

وللإجابة على هذه الإشكالية ارتأينا تناول هذا الموضوع من خلال محورين اثنين هما على الشكل التالي:

المحور الأول: إساءة استخدام النظام المعلوماتي في ارتكاب الجرائم الالكترونية

تدخل الجرائم المرتكبة عبر الأنترنيت أو الجرائم المعلوماتية في إطار دراسة القانون الجنائي الداخلي (الوطني)، حيث تعد من الجرائم التي تتخطى حدود الدولة الواحدة، فهي تدخل أيضا في نطاق دراسات القانون الجنائي الدولي وتدخل كذلك في إطار الجريمة المنظمة التي تقوم على أساس تنظيم هيكلي وتدريجي له صفة الاستمرارية لتحقيق مكاسب طائلة.) الشوابكة، 2004(

فإساءة استخدام المعلوميات واستغلالها على نحو غير مشروع، أدى إلى ظهور طائفة جديدة من الجرائم عرفت بالجرائم المعلوماتية (فرام، 2009) التي تعد من الموضوعات الحديثة التي فرضت نفسها على المستوى الوطني والدولي على حد سواء (العجمي، 2015، صفحة 3)، فقد أضحت اليوم تفرض نفسها بقوة على التشريعات الجنائية بالنظر على الطابع الخاص الذي تمتاز به في علاقتها بباقي الجرائم التقليدية ذلك ان من اهم خصوصياتها انها ترتكب في عالم افتراضي وتعتمد عل آليات افتراضية بل وقد تكون أهدافها افتراضية كما هو الحال بالنسبة لجرائم المس بنظم المعالجة الآلية للمعطيات التي تتم سواء عن طريق الدخول الى هذه الأنظمة بطريقة غير مشروعة أو من خلال إحداث تغييرات عليها بالحذف أو التغيير أو الاتلاف، الأمر الذي دفع المشرع الجنائي المغربي إلى سن مقتضيات خاصة تهم مكافحة هذا الصنف من الجرائم عبر مجموعة من القواعد المنصوص عليها في القانون 07-03.

فانتشار شبكات الاتصال والمعلومات ودخول تطبيقاتها في بيئة المجتمعات المعاصرة ساهم في تعزيز التواصل، إلا أنها في المقابل ساعدت في شيوع الجريمة بمختلف أشكالها، حيث قدمت هذه الوسائل تسهيلات كبرى للأنشطة الإجرامية المنظمة والفردية، جاعلة الأمن الاقتصادي والاجتماعي لكثير من الدول عرضة لأنماط جديدة من الجرائم الذكية تتباين ما بين الاستعمال غير المشروع لبطائق الائتمان (أولا)، والاعتداءات المهددة للأنظمة المعلوماتية (ثانيا).

أولا-الاستعمال غير المشروع لبطائق الائتمان:

إن التعامل بالبطائق البنكية وإن كان حديث العهد نسبيا، إلا أن انتشارها وتزايد التعامل بها صاحبه نموا متزايدا في الجرائم المصاحبة لاستخدامها، حيث احترف البعض سرقة هذه البطائق أو استخدامها بالتحايل في الاستيلاء على مال الغير، فقد طرح استعمالها من الغير استعمالا غير قانوني عدة إشكاليات على مستوى العمل القضائي، بالنظر إلى تكييفها فأحيانا تدخل ضمن جرائم الأموال، وأحيانا أخرى ضمن جرائم تزوير المحررات، ويمكن قسيمها إلى عدة أنواع منها: بطاقة السحب الآلي (الشافعي، 2002)، بطاقة الوفاء، بطاقة الضمان، بطاقة الائتمان.

فالاستعمال غير المشروع للبطاقة بواسطة الغير، لا يتم من خلاله خرق شرعية البطاقة، فهي صحيحة ودخلت حيازة الغير نتيجة السرقة او الفقد، وإنما يتم خرق شرعية الحامل فالاستيلاء على أرقام بطائق الائتمان وتداولها بين العديد من الأشخاص واستعمالها (البختي، 2004)، فإذا قام شخص باختلاس بطاقة ائتمان واتجهت نيته إلى تملكها فإنه يعد مرتكبا لجريمة السرقة، أيا كان الباعث الذي دفعه لذلك فتقوم جريمة السرقة ولو كانت نية المتهم متجهة إلى مجرد الاحتفاظ بها وحرمان حاملها من استعمالها.

إلا أن هناك إشكالا قانونيا يطرح ويتعلق بالوضع القانوني للدفع الإلكتروني بالبطاقة الائتمانية في شبكة الأنترنت من قبل شخص غير صاحب الحساب البنكي؟

ويثور إشكال آخر متمثل فيما إذا كانت بطائق الائتمان تستلزم وجوب حمايتها جنائيا للحيلولة دون وقوع اعتداء عليها، خصوصا وأنها تشكل جانبا من المعاملات المالية والتجارية في الوقت الحالي فهل من المتصور أن تكون محلا لجريمة النصب؟

لكن في حالة استعمال بطاقة الائتمان من قبل شخص غير مالكها بعد قيامه بسرقتها أو تزويرها في إجراء عملية سحب للنقود من الموزع الآلي بالبنك، فهل يعتبر ذلك نصبا؟ وهل يمكن خداع الجهاز الآلي خصوصا وأنه يشرف عليه مستخدم بالبنك وبالتالي إيقاعه في الغلط، مادام أن ساحب النقود بواسطة البطاقة المسروقة أو المزورة يظهر بمظهر مالكها الشرعي؟

جوابا على هذا الإشكال، فإن استعمال شخص آخر غير مالك البطاقة في الاستيلاء على أموال الجهة المصدرة لها بدون وجه حق لا يسمح بانطباق وصف جريمة النصب على سلوك الجاني في هذه الحالة، وإنما يكون جريمتي السرقة والتزوير، وذلك على أساس أن الجاني قد استولى بدون وجه حق على أموال غير مملوكة له وبدون رضاء حائزها الشرعي، وهو ما يدخل في نطاق جريمة السرقة، كما أنه يكون قد حصل على الأموال عن طريق التلاعب في البيانات المخزنة بالبطاقة مما يعد تزويرا لها، ونكون بصدد تعدد للجرائم شريطة أن يكون تزوير البيانات المعالجة آليا معاقبا عليه بنصوص حديثة (فرام، 2009، صفحة 44).

ثانيا- المس بالأنظمة المعلوماتية:

اتخذت الجريمة المعلوماتية في المملكة المغربية خلال العقود الأخيرة صورا متعددة، مما دفع المشرع إلى سن تشريع مهم، لكونه صدر لسد الفراغ التشريعي في مجال مكافحة الجرائم المعلوماتية، وهو القانون رقم 03-07 بشأن تتميم مجموعة القانون الجنائي فيما يتعلق بالإخلال بسير نظم المعالجة الآلية للمعطيات، ويحتوي هذا القانون على تسعة فصول (من الفصل 3-607 إلى الفصل11-607 من مجموعة القانون الجنائي المغربي). وأول ما يلاحظ هو عدم قيام المشرع المغربي بوضع تعريف لنظام المعالجة الآلية للمعطيات، ويبدو أن المشرع قصد ذلك، بحيث ترك ذلك للفقه والقضاء، هذا الأخير المكلف بتطبيق بنود هذا التشريع، ثم إن المجال المعلوماتي هو مجال حديث ومتجدد، وبالتالي فإن أي تعريف يتم وضعه قد يصبح متجاوزاً فيما بعد، في ضوء التطور المذهل لقطاع تكنولوجيات الاتصالات والمعلومات، وعليه، فقد أحسن المشرع المغربي عند عدم وضعه لتعريف خاص بنظام المعالجة الآلية للمعطيات. وعند رجوعنا للقانون الفرنسي مثلا بشأن الغش المعلوماتي لسنة 1988، نلاحظ أن هذا التشريع كذلك لم يحدد مفهوم نظام المعالجة الآلية للمعطيات، بل اقتصر على بيان أوجه الانتهاكات المتعلقة بهذا النظام وعقوباتها.

وتجدر الإشارة إلى أن تدخل المشرع المغربي لتميم مجموعة القانون الجنائي بمقتضيات مجرمة لمختلف الأفعال الجرمية الماسة بنظم المعالجة الآلية للمعطيات وذلك بمقتضى القانون رقم 07.03 لسنة 2003 قد انبنى على ثلاثة أسباب رئيسية وهي:

- ✓ مواءمة مجموعة القانون الجنائي مع المقتضيات التي أتى بها القانون المتعلق بمكافحة الإرهاب، بحيث تم تضمين اللائحة المنصوص عليها بالفصل 218-1 الذي أضيف لمجموعة القانون الجنائي بمقتضى قانون مكافحة الإرهاب، الجرائم المتعلقة بنظم المعالجة الآلية للمعطيات باعتبارها أفعالا إرهابية إذا كانت لها علاقة عمدا بمشروع فردي أو جماعي يهدف المس الخطير بالنظام العام بواسطة التخويف أو الترهيب أو العنف، والحال أن مقتضيات المجموعة الجنائية لم تكن تتضمن آنذاك فصولا خاصة بالجرائم الماسة بنظم المعالجة الآلية للمعطيات وبالتالي كان المشرع ملزما إلى حد ما بإصدار قانون 07.03 من أجل المواءمة والتناسق في مقتضيات مجموعة القانون الجنائي.
- ✓ ملء الفراغ الذي كانت تعرفه مجموعة القانون الجنائي في هذا الإطار، والذي خلق عدة إشكالات عملية بالنسبة للقضاء المغربي الذي وجد نفسه عاجزا في العديد من النوازل على إيجاد أساس قانوني للمتابعة والمؤاخذة وتطبيق العقاب الملائم على مرتكبي الأفعال الجرمية المشكلة لبعض صور الجريمة المعلوماتية بحيث تم في حالات عدة تبرئة مرتكبي بعض هذه الأفعال استنادا لمبدأ الشرعية القانونية الذي يفرض عدم مؤاخذة أحد على فعل لا يعد جريمة بصريح القانون ولا معاقبته بعقوبات لم يقررها القانون.
- ✓ مواءمة التشريع الجنائي المغربي مع الاتفاقيات الدولية والإقليمية ومع مواقف التشريعات الأوروبية وخاصة التشريع الفرنسي، بحيث استفاد المشرع المغربي كثيرا من التطور التشريعي والقضائي الذي عرفته فرنسا في هذا الصدد.

وعموما لا تخرج صور الجريمة المعلوماتية التي تم تجريمها بمقتضى قانون 07.03 عن أربعة صور رئيسية يمكن أن تأتي مترابطة فيما بينها أو مستقلة عن بعضها البعض بحيث يكفي لتوقيع العقوبات المقررة لها ارتكاب إحدى هذه الصور فقط أو فعل من الأفعال المكونة لها، ويمكن حصر هذه الأفعال في الجرائم التالية:

- ✓ الدخول الاحتيالي على مجموعة أو بعض نظام للمعالجة الآلية للمعطيات.
- ✓ البقاء في نظام للمعالجة الآلية للمعطيات بعد الدخول خطأ فيه.
- ✓ حذف أو تغيير المعطيات المدرجة في نظام المعالجة الآلية للمعطيات أو التسبب في اضطراب في سيره.
- ✓ العرقلة العمدية لسير نظام المعالجة الآلية للمعطيات أو احداث خلل فيه.
- ✓ ادخال معطيات في نظام للمعالجة الآلية للمعطيات أو اتلافها او حذفها منه أو تغيير المعطيات المدرجة فيه، أو تغيير طريقة معالجتها أو طريقة ارسالها بشكل احتيالي.
- ✓ التزوير أو التزييف لوثائق المعطيات أيا كان شكلها إذا كان من شأن التزوير أو التزييف الحاق ضرر بالغير.
- ✓ استعمال وثائق معلوميات مزورة أو مزيفة.
- ✓ صنع تجهيزات أو أدوات أو اعداد برامج للمعلوميات أو أية معطيات أعدت أو اعتمدت خصيصا لأجل ارتكاب هذه الجرائم أو تملكها أو حيازتها أو التخلي عنها للغير أو عرضها رهن إشارة الغير.
- ✓ محاولة ارتكاب الجرائم المذكورة.
- ✓ المشاركة في عصابة أو اتفاق لأجل الاعداد لواحدة أو أكثر من هذه الجرائم.

وتجدر الإشارة إلى أن الوسائل الإلكترونية أصبحت تشكل سلاحا في يد بعض الأفراد والجهات، والتي تهدد من خلالها السلم والأمن، وبالتالي كان لابد من تدخل المشرع للحد من هذه الخطورة خصوصا عندما يتعلق بجرائم إرهابية تمس حياة الأفراد والاستقرار، وسن قوانين زجرية ضمنها في مجموعة القانون الجنائي، وهو ما ستراه من خلال التطرق بشكل مقتضب لصور الجريمة الإلكترونية في القانون رقم 03.03 (الإرهاب، 2003)المتعلق بالإرهاب، والقانون رقم 24.03 المتعلق بتعزيز الحماية الجنائية للطفل والمرأة.

➢ صور الجريمة الإلكترونية في القانون رقم 03.03: يمكن القول بأن هذا القانون يعتبر أول قانون تمت الإشارة فيه بشكل صريح للإجرام الإلكتروني كوسيلة لارتكاب أفعال إرهابية لها علاقة عمدية بمشروع فردي أو جماعي، يهدف إلى المس بالنظام العام بالتخويف أو الترهيب أو العنف، بحيث أن الفصل 218-1 قد حدد على سبيل الحصر الجرائم المتعلقة بنظم المعالجة الآلية للبيانات أو المعطيات، لكن ثار التساؤل حول الأساس القانوني لهذه الجرائم، الشيء الذي دفع بالمشرع إلى الإسراع لتبني قانون خاص بهذا النمط الجديد من الجرائم وهو ما جسده القانون رقم 07.03 المتعلق بسير نظم المعالجة الآلية للمعطيات المذكور سلفا.

وبالرجوع إلى ذات الفصل نجده يعاقب على كل تزوير أو تزييف للشيكات أو أية وسيلة أخرى للأداء تمت الإشارة إليها في المادتين 316[1] و331من مدونة التجارة المغربية، كما عاقب على الإشادة بالأعمال الإرهابية بواسطة وسائل الإعلام ومنها الإلكترونية حيث حدد عقوبتها في الحبس من سنتين إلى ست سنوات وبغرامة من 10.000 إلى 500.000 درهم حست الفصل 2018-2.

➢ القانون رقم 24.03 المتعلق بتعزيز الحماية الجنائية للطفل والمرأة (برزجو، صفحة 69): هذا القانون قد خص لهذا النوع من الجرائم المعلوماتية فصلين اثنين هما الفصل 503-1 والفصل 503-2 حيث عاقب الفصل الأول على جريمة التحرش الجنسي الذي لم يكن مجرما، فقد جاء هذا الفصل بصيغة يمكن معها إدراج التحرش الجنسي الذي يقع عبر وسائل الاتصال الحديثة ضمنها، وعاقب مرتكب هذا الفعل بالحبس من سنة إلى سنتين وغرامة من خمسة آلاف إلى خمسين ألف درهم.

أما فيما يتعلق بالتحريض أو التشجيع أو تسهيل استغلال الأطفال الذين تقل سنهم عن 18 سنة في المواد الإباحية التي تستخدم فيها الوسائل المعلوماتية، فخصص لهذه الأفعال عقوبة تصل من سنة إلى سنتين حبسا وغرامة من خمسة آلاف إلى خمسين ألف درهم طبقا لمقتضيات الفصل 503-2 من مجموعة القانون الجنائي.

ويجب التنويه بما قام به المشرع المغربي من تعزيز الحماية للطفل من النشرات أيا كان نوعها، المعدة للبغاء أو الدعارة أو الإجرام أو الاستهلاك أو ترويج المخدرات والمؤثرات العقلية أو الكحول أو السجائر، من خلال مقتضيات القسم الثالث، حيث عاقب بغرامة تتراوح بين 100.000 إلى 500.000 درهم كل من عرض نشرات إلكترونيا أو في الطريق العمومية أو خارج المتاجر أو قام بالدعاية لما سبق.

المحور الثاني: النظام المعلوماتي موضوع الجريمة المعلوماتية بين قواعد التشريع والاجتهاد القضائي

إن النصوص القانونية تضل جامدة حتى إذا خرجت إلى حيز التطبيق العملي ظهرت عيوبها ونواقصها الأمر الذي يؤثر على توجه القضاء أثناء الفصل في المنازعات المتعلقة بمجال تدخل تلك النصوص فقد عرضت على القضاء المغربي مجموعة من القضايا التي تتعلق بالجريمة المعلوماتية لكنه آنذاك واجه بعض الإشكالات أهمها الفراغ التشريعي في مجال مواجهة هذا النوع من الجرائم، وحتى لا يفلت الجاني من العقاب فقد ترك الأمر للقضاء لكي يقول كلمته لسد النقص التشريعي رغم ما ينطوي عليه ذلك من انتهاكات لمبدأ الشرعية، إلا أنه بصدور القانون رقم 03.07 استغل المشرع المغربي فرصة إصدار تشريع معلوماتي يجرم مجموعة من الأفعال ويمكن للقضاء بموجبها متابعة الجاني.

غير أن ما تجدر الإشارة إليه هو أن التطبيقات القضائية لمقتضيات القانون رقم 07.03 المتعلق بتنظيم المعالجة الآلية للمعطيات المذكور سابقا تواجه صعوبات وإكراهات كبيرة وذلك راجع بالأساس إلى تأخر المشرع المغربي في التصدي للجرائم الإلكترونية على الجرائم من ظهورها وبداية انتشارها وتوسيع مجالات ارتكابها، الأمر الذي انعكس على التوجه القضائي حيث انقسم على أنفسه إلى رأيين، الأول منه يسير في اتجاه اعتماد القواعد العامة كأساس قانوني لإدانة مرتكبي هذا الصنف من الجرائم وذلك من خلال تكيفات مختلفة خاصة السرقة وخيانة الأمانة والنصب والاحتيال، وقدساير في ذلك نظيره الفرنسي الذي سبق له أن طبق جريمة السرقة على برامج المعلوماتية على غرار سرقة التيار الكهربائي (بنسليمان، 2017)

في حين يرى اتجاه ثاني أن الجريمة المعلوماتية صنف خاص يقتضي قواعد خاصة ولا يمكن بأي حال من الحوال إخضاعه للقواعد العامة اقتداء بالتوجه التشريعي الجديد الذي صبغ قوانين الجديدة من الدول، وقد تغلب الاتجاه الأخير الذي كان له صدى على أكثر من مستوى، خاصة بعد صدور القانون رقم 03-07 المتعلق بالمس بنظم المعالجة الآلية للمعطيات.

إلا أن الاتجاه الأخير قد عانا كثيرا في بداية تطبيق مقتضيات القانون رقم 03-07 فيما يخص استيعاب مفهوم نظام المعالجة الآلية للمعطيات، وذلك من خلال صعوبة تحديد مجال ونطاق هذا النظام، وهو ما انعكس سلبا على إشكالية التطبيق القانوني للأفعال موضوع المتابعة وذلك بالنظر إلى التطور الهائل والسريع الذي يعرفه الأجرام المعلوماتي نظرا لخصوصية الفضاء الرقمي ولتنوع واختلاف بيئة الجريمة.

وعليه، فهل استقر العمل القضائي المغربي على رؤية موحدة في معالجته للإشكالات التي تطرحها ظاهرة الإجرام المعلوماتي؟ وإذا كانت التطبيقات القضائية غير مستقرة في هذا المجال، فهل ذلك راجع لصعوبة الإحاطة بهذا النوع من الجرائم من قبل رجال القضاء أم أن النصوص القانونية لم تستوعب جميع مظاهر الجريمة المعلوماتية؟ الشيء الذي سنحاول توضيحه من خلال النقط التالية:

أولا: القضاء المغربي بين إشكالية المفهوم وصعوبة تحديد نطاق المعالجة الآلية

لقد انعكس التأخير التشريعي على موقف القضاء خاصة عند تطبيق مقتضيات القانون رقم 03.07 فيما يتعلق بتحديد مفهوم نظام المعالجة الآلية للمعطيات وتحديد نطاقه، حيث بأن تحديده اتسم بالارتباك والقصور في استيعاب

مفهوم نظام المعالجة الآلية للمعطيات، وخير مثال على ذلك التناقض الذي واجهته المحاكم المغربية بخصوص البريد الإلكتروني وما إذا كان نظاما للمعالجة الآلية للمعطيات أم لا، حيث طرحت أولى القضايا المرتبطة بالبريد الإلكتروني سنة 2007 على المحكمة الابتدائية بالدار البيضاء، التي رفضت اعتبار الإيميل آنذاك نظاما للمعالجة الآلية للمعطيات، لكن بعد ذلك استقرت المحاكم المغربية على اعتبار البريد الإلكتروني نظاما للمعالجة الآلية للمعطيات، وهذا ما ذهبت إليه محكمة الاستئناف بالرباط في أحد قراراتها (19/2010/751، 2012).

فأصبحت الأحكام الصادرة عن مختلف المحاكم المغربية تعتبر أن البريد الإلكتروني يدخل ضمن نظام المعالجة الألية للمعطيات، ونستحضر في هذا الصدد الحكم الصادر عن ابتدائية تمارة في نفس السنة (ماي 2010) ، إلى غيرها من الأحكام التي تصب في هذا المنوال.

وعليه يمكن القول بأن القضاء المغربي كان يرفض اعتبار الإيميل نظام من نظم المعالجة الألية للمعطيات، ولعل ذلك راجع إلى البداية الأولى لتطبيق أحكام القانون رقم 07/03 والتردد في التعامل مع هذه التقنية الجديدة على القضاء في تلك المرحلة، إلا أنه تدارك الموقف بعد ذلك وأصبح يعتبرها ضمن النظام بفضل شيوع اعتمادها في ارتكاب جرائم المس بنظم المعالجة الألية للمعطيات، وخاصة تلك المرتبطة بالدخول الاحتيالي وفقا لمقتضيات المادة 607-3 من القانون الجنائي.

وهكذا أوضح ثبات التوجه القضائي في اعتبار البريد الإلكتروني (الإيميل) نظاما للمعالجة الألية للمعطيات، فقد كان لزاما على المحاكم المغربية مسايرة التطور التكنولوجي في هذا الإطار، وذلك من خلال التصدي لكل القضايا المستجدة في الموضوع كما هو الشأن بالنسبة للهاتف النقال مثلا، حيث نستشف من خلال تتبعنا لتجربة الاجتهاد القضائي في الموضوع أنه قد أدخل ضمن نظم المعالجة الألية للمعطيات الهاتف النقال، فبعد الحكم الصادر عن المحكمة الابتدائية بالرباط والتي اعتبرت أن الهاتف المحمول يدخل ضمن نطاق أنظمة الحماية الألية للمعطيات.

ومن القضايا المستجدة التي أضحت تعرض على المحاكم بحدة تلك الجرائم المرتبطة بالموقع الاجتماعي (فيسبوك، توتير) حيث يكثر التساؤل التالي هل تعتبر هذه الأخيرة نظاما للمعالجة الألية للمعطيات أم لا؟ وفي ظل غموض النص التشريعي وغياب وضع لائحة من قبل القضاء على غرار مت قام به القضاء الفرنسي كما أشرنا إلى ذلك أعلاه وهو الأمر الذي أسهم في إرباك التوجه القضائي عند بروز هذه القضايا في شكل دعاوى أمام المحاكم المغربية، ويمكن أن نستشهد في هذا الصدد ببعض الأحكام المهمة الصادرة عن المحكمة الابتدائية بالرباط لرصد كيف وقع التطور الإيجابي في اعتبار مواقع التواصل الاجتماعي تدخل في إطار نظم المعالجة الألية للمعطيات (حكم صادر عن المحكمة الابتدائية عدد ملف رقم 2105/1666/2012 بتاريخ 2012/10/18 حكم رقم 855 ملف جنحي تلبسي عدد 2015/869/2014 بتاريخ 2014/05/26 المحكمة الابتدائية بالرباط).

وبالرجوع إلى هذه الأحكام نلاحظ أن المحكمة الابتدائية بالرباط لم تكن تعتبر أن مواقع التواصل الاجتماعي تدخل ضمن أنظمة المعالجة الألية للمعطيات وهو ما يمكن أن نستشفه من خلال حكمين صادرين عنها في الموضوع، الأول كان سنة 2012 بحيث تتلخص وقائع القضية في كون المتهم وقتا كانا يتبادلان الدردشة عبر الفيس بوك إذ بلغ بهم الحال إلى تبادل الصور خليعة احتفظ المتهم بها، ولما رفضت الفتاة الزواج به لظروف خاصة هددها بنشر تلك الصور إذا لم تعطيه مبلغ 10.000 درهم بل قد نجده بدأ فعلا بتهديده بنشر صورتين لها (حكم صادر عن المحكمة الابتدائية

عدد ملف رقم 2105/1666/2012 بتاريخ 2012/10/18.)، أما الحكم الثاني فقد صدر بتاريخ 2014، وقد ذهب الحكم الأخير إلى القول بأن نشر صور إباحية على موقع التواصل الاجتماعي فيس بوك يدخل ضمن مقتضيات الفصل 490 من القانون الجنائي والفقرة الأخيرة من هذا الفصل 59 من ظهير 15 نونبر1958، وبالتالي لم يعتبر الحكم أن تلك الأفعال تدخل ضمن الفصول من 607-3 إلى 607-11 من القانون الجنائي/ وهو ما يستشف من خلال قراءة مضامين الحكم (حكم رقم 855 ملف جنحي تلبسي عدد 2015/869/2014 بتاريخ 2014/05/26 المحكمة الابتدائية بالرباط.)، إلا أنه بعد ذلك تداركت ذات المحكمة في أحدث أحكامها واعتبرت أن الفيس بوك يدخل ضمن نظام المعالجة الألية للمعطيات وطبقت عليه أحكام الفصلين -607-3 و 307-6 من القانون الجنائي.

ونحن إذا نساير المحكمة في توجهها، إلا أنه يجب التفريق بين الحالة التي تكون فيها مواقع التواصل الاجتماعية قيمة أما بكلمة سر أو بشرط من الشروط التي يعرفها صاحب الموقع، ولكن مع ذلك تم التلاعب والعبث بالمعلومات والبيانات الواردة فيه، هنا نكون أمام جريمة الدخول الاحتيالي معقب عليها طبق للقانون في الفصل 607-3.

ومرد هذا التباين في تحديد العناصر التي يمكن أن يشملها نظام المعالجة الألية للمعطيات يرجع أساسيا إلى عدم وضع تعريف محدد ومنضبط لهذا النظام من قبل أغلب التشريعات، ومن بينها التشريع المغربي وهو ما دفع محكمة الاستئناف بالرباط إلى تعريف النظام بأنه «كل مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج، وأجهزة الربط التي تربط بينها مجموعة من العلاقات التي عن طريقها يتم تحقيق نتيجة معينة ، وهي معالجة المعطيات أو التي تتظاهر فيما بينها نحو تحقيق نتيجة معينة، وهي معالجة معطيات على أن يكون هذا المركب خاضعا لنظام الحماية الفنية".

وهو نفس التعريف الذي أعطاه مجلس الشيوخ الفرنسي أثناء مناقشته لمشروع القانون المتعلق بالغش المعلوماتي (la froud informatique)الذي دخل حيز التطبيق بداية من سنة 1988 والذي أدخلت عليه عدة تعديلات هامة كان أخرها بتاريخ 2015/07/24 ، وبذلك يكون مواكبا لتطور السريع الذي يعرفه عالم التكنولوجيا المعلوماتية في حين بقي المشرع المغربي حبيس القانون 07.03 بدون تعديل والتعريف الذي تبنته محكمة الاستئناف في حاجة إلى مراجعة وذلك لسببين هو أن الغرفة الجنائية بمحكمة النقض في فرنسا أعطت مفهوما واسعا لنظام المعالجة الألية للمعطيات، وهو ما سبق أن أشرنا إليه أعلاه، أما السبب الثاني فهو أن التعريف الذي جاء به مجلس الأعلى للشيوخ الفرنسي أثناء الأشغال التحضيرية لقانون 1988 أصبح متجاوز حيث حرص مجلس الشيوخ في هده المرحلة على ربط القانون الجنائي بالتقدم التكنلوجي.

والواقع أن هذا التذبذب والارتباك في موقف القضاء المغربي لم يقتصر على مفهوم نظام المعالجة الآلية للمعطيات وإنما امتد أيضا الى تحديد المفاهيم المرتبطة بعناصر الجرائم موضوع الدراسة ويبرز هذا التذبذب خصوصا في صور الولوج الى أنظمة المعالجة الآلية للمعطيات، ومن صور الولوج أيضا الدخول الى شبكة الأنترنيت وذلك باستخدام الأمن الإلكتروني الخاص بإحدى الدول الأجنبية البحث عن استمارات الزبناء المنخرطين لدى البنوك

وإرسالهم أليهم لملئها وإعادتها ليقوم الجناة باستغلال المعطيات التي دونها الزبناء في الاستمارات وتحويلها الى بطاقات ائتمان مع الاحتفاظ بالرقم السري الخاص بالمنخرطين واستغلاله في سحب النقود من الشبابيك البنكية.

والولوج في نظرنا لا يقتصر على الحالات المعروضة على القضاء فقط بل يمتد الى صور أخرى قد تعرض على القضاء ليقول كلمته فيها، وإعطاء التكييف الصحيح للأفعال التي تدخل في إطار قانون المس ينظم المعالجة الآلية للمعطيات من تلك التي تدخل فيه، حيت قد يتعرض الزبناء غالبا الى مصائد ومكائد في شكل نصب وتدليس، وتجدر الإشارة إلى أن تحديد معنى الاحتيال أو التحايل يترك لقاضي التحقيق الموضوع في ظل القواعد المعتمدة في تفسير النصوص كما هو الشأن بالنسبة الى الاطلاع الغير مصرح به على المعلومات المخزنة في ذاكرة الحاسب الآلي، والذي يأخذ بدوره صورا عديدة منها سرقة القائمة والاطلاع أو قراءة المعلومات أو مجرد التصنت على المعلومات البسيطة (سليمان، 2017)، من جهة أخرى يمكن ملامسة جريمة الولوج عن طريق الاحتيال إلى نظام المعالجة إلى نظام المعالجة الآلية للمعطيات عن قرب من خلال استعمال بطائق ائتمان مزورة، وهو ما نلمسه من خلال تتبع بعض القضايا المرتبطة بالموضوع، منها على سبيل المثال ما قام به المتهمان في القضية المعروفة بفيروس zotob عندما اعترف بأنهما " ولجا أنظمة المعالجة الآلية للمعطيات واستعمالا بطاقة ائتمان مزورة واستولى كل منهما بواسطة ذلك على مبتغاه المالي على فترات متتالية ولمدة معينة ...، وكذا توصل أحدهما بمجالات اشهارية وملابس شخصية."

يبدا أن المحكمة لم تعتبر في قرار آخر صادر عنها في قضية مماثلة أن ما قام به المتهمون من استعمال أرقام بطاقات ائتمان مزورة عبر الانترنيت والاستيلاء على أموال عدد من الضحايا بنفس الطريقة ولوجا الى انظمة المعالجة الآلية للمعطيات عن طريق الاحتيال بل لم تعتبره حتى جريمة النصب كما ذهبت النيابة العامة في متابعتها معللة قرارها بأن المتهمين لمن يكن لهم أي اتصال بالضحايا وأعادت المحكمة التكييف على أساس ذلك معتبرة أن ما قام به المتهمون يشكل جريمة سرقة موصوفة.

والواضح أن النيابة العامة كانت مقصرة لأنها لم تتابع المتهمين بجريمة الولوج عن طريق الاحتيال طبقا للفقرة الاولى من الفصل 607-3 من القانون الجنائي من جهة وعلى احجام وتلكؤ المحكمة عن اعادة تكييف الفصية من جهة أخرى، ففي المثال الاخير عندما ينتج عن الدخول الى النظام عرقلة أو تغيير أو حذف للمعطيات فإننا نكون أمام تعدي الجريمة الالكترونية أو جريمة المس بنظام المعالجة الالية للمعطيات إلى جريمة أو جرائم أخرى من جرائم الأموال وهو ما يجعلنا أمام جريمتين مستقلتين بعناصر هما، فنرجع في هذه الحالة الى 607-3 الفقرة الثالثة من القانون الجنائي من أننا نشدد العقوبة إذا نتج عن الدخول مس بسلامة وأمن المعطيات، باعتباره قانونا خاصا في الوقت الذي ينتج عن هذه العملية ضياع لقواعد بيانات أو أموال كثيرة جد مهمة تصل إلى ملايير الدراهم.

فبالرجوع الى الفصل 607-3 فقرة 3 من ق/ج نجده يشدد العقوبة والتي لا يتجاوز في حدها الأقصى سنتين والحل في نظرنا أن قاضي الموضوع يجب أن يتعامل مع كل قضية على حدى بحسب وقائعها وملابساتها تطبيقا لمبدأ تفريد الجزاء الجنائي والذي يأخذ بعين الاعتبار جسامة الفعل الجنائي والفعل دون إغفال الخطورة الاجرامية للجاني (بنسليمان، 2017، صفحة 122)، وهذا من أن يتدخل المشرع لمعالجة هذه النقطة والوقوف على نية المتهم الذي يقصد من وراء عملية الحذف أو التغيير الحصول عل أموال طائلة أو أشياء ذات قيمة مهمة كما أوضحت بعض

التشريعات ومنها التشريع الألماني وبعض الولايات الأمريكية كولاية "تينسي" التي نصت على الدخول الاحتيالي والحصول على مبالغ مالية.

وفي نفس السياق كان حريا بالقضاء المغربي أن يحذو حذو نظيره الفرنسي الذي اعتبر أن الدخول عن طريق الاحتيالl'accès frauduleux المنصوص عليها في المادة 323-1 من القانون الجنائي الفرنسي يشمل جميع أنواع الدخول الغير مشروع الى نظم المعالجة الالية للمعطيات ولو كان الشخص الذي قام بالولوج يشتغل على نفس الجهاز لكن على نظام آخر سواء تم الولوج عن بعد أو كان مرتبطا بخط الاتصال ويتحقق ذلك إذ كان حق الاطلاع على البيانات مقصورا على أشخاص أو هيئات معينة ليس من بينهم الجاني.

ثانيا: العمل القضائي وأزمة دينامية الإجرام المعلوماتي:

من خلال استقراء الأحكام والقضايا السابقة على المحاكم، وبالنظر إلى موقف القضاء المغربي منها يلاحظ أنها تنحصر فقط في جريمة الدخول الاحتيالي التي تعتبر أم الجرائم، فقد لاحظنا من خلال استعراضنا للأحكام تذبذبا في مواقف القضاء، الشيء الذي يعود لصعوبة تكييف الجرائم وخاصة الجرائم غي منصوص عليها في القانون 07-03 وإشكالية التطبيق العملي.

فتنوع الجريمة المعلوماتية وتطور أساليب ارتكابها انعكس على نوعية القضايا المعروضة على المحاكم، حيث يلجأ مقترفو الجرائم الى أساليب جد متطورة وتقنية عالية لا نجدها في الجرائم العادية من قبيل ذلك تجاوز الحواجز الأمنية التي تضعها بعض الأنظمة المعلوماتية حماية لها من اختراقات القراصنة والتلاعب بالمهندسين الساهرين على تأمين المواقع الالكترونية إذ يتم التحكم والاستئثار بالخادم الرئيسي ويتم استغلال حيز من المواقع الالكترونية بعد وضعهم اليد على الثغرات الموجودة على مستوى تأمين المواقع المستهدفة.

ومن صور الاحتمال أيضا استخدام ما يعرف ب PRORAT الذي يمكن من الدخول الى أجهزة الأشخاص المتراسل معهم (**حكم ابتدائي عدد 37 صادر بتاريخ 2006/08/06 عن المحكمة الابتدائية بالدار البيضاء.**)، وما يؤيد هذا الطرح ما ذهبت المحكمة الابتدائية بالقنيطرة في حيثيات أحد أحكامها عندما قام شخص بالولوج الى نظام المعالجة الالية للمعطيات بشركة تحويل الاموال "مونيغرام" والاستيلاء على مبلغ مالية بعثها الى عدة أشخاص أغلبهم فتيات مما تكون معه جنحة النصب المنصوص عليها وعلى عقوبتها في الفصل 540 من القانون الجنائي المغربي قائمة العناصر باستخدامه مستندات عير صحيحة واستيلائه على مبالغ مالية بغير وجه حق، وحيت إن المتهم ولج الى نظام المعالجة الآلية للمعطيات عن طريق الاحتيال ولم يكتف ذلك بل عمد الى إحداث تغييرات بهذا النظام مكنته من خرق حوالات وهمية سلم أرقامها السرية الى عدة أشخاص منهم المتهمين ليعملوا على استخلاصها من وكالة تحويل الاموال مما يكون معه عناصر الفعل المنصوص عليها في المادة 607-3 من القانون الجنائي متوفرة، والتي يجرم فعل الدخول عن طريق الاحتيال وتضاعف العقوبة إذا نتج عن هذا الدخول حذف أو تغيير للمعطيات وهو الحاصل في نازلة الحال"

وعليه فالمحكمة لم تبين العناصر التكوينية لجريمة الولوج الى أنظمة المعالجة الآلية للمعطيات، واكتفت باعتبار الدخول الى الموقع الالكتروني لشركة تحويل الأموال "مونيغرام" ولوجا الى أنظمة المعالجة الآلية للمعطيات الخاصة

بهذه الشركة دون أن تحدد كيف تم الولوج الى داخل النظام، وما هو وجه الاحتيال فيه إذ من المعلوم أن شركات تحويل الاموال تقوم بنقل أو تحويل الاموال من جهة إلى أخرى بناءا على طلب الزبون الذي يجب عليه أن يدفع المبلغ المالي المراد تحويله، وكذا مصاريف عملية تحويله الى الجهة التي يريدها، ودخول أحد الاشخاص الى الموقع الالكتروني لشركة وطلب تحويل الاموال ليس مجرما في حد ذاته وإنما استعماله لوسائل الاحتيال قصد الولوج هو الفعل المجرم وهذا ما كان يجب على المحكمة بيانه في حيثياتها، وفي نفس الإطار ذهبت محكمة الاستئناف بالرباط الى اعتبار استعمال بطاقات ائتمان مزورة عن طريق إيلاجها في الشباك الاوتوماتيكي واستخراج النقود بمثابة احتيال في الولوج الى المعالجة الآلية للمعطيات (عن غرفة الجنايات الابتدائية بمحكمة الاستئناف بالرباط ملحقة حي السلام، ملف عدد 22/05/447، أيده قرار من طرف الجنايات الاستئنافية بنفس المحكمة بتاريخ 2006/10/04 ملف عدد 26/06/807).

ويلاحظ أن المحكمة لم تميز في القرار الأخير بين جريمة استعمال بطاقات ائتمان مزورة والولوج الى المعالجة الآلية للمعطيات عن طريق الاحتيال وهما جريمتان مستقلتان تنفرد كل منهما بعناصرها المادية حيث اعتبرت المحكمة أن استعمال البطاقة المزورة أي إدخالها في الشباك الأوتوماتيكي وسحب النقود ولوجاً إلى أنظمة المعالجة الآلية للمعطيات عن طريق الاحتيال (بنسليمان، 2017، صفحة 126)، في حين نجد أن محكمة الاستئناف بالرباط اعتبرتها جريمة مستقلة وتكيفها على هذا الاساس دون الالتفات الى اعتبارها ولوجا إلى أنظمة المعالجة الآلية للمعطيات (من القرارات الصادرة عنها، من بينها قرار المشار الى عدده صدر بتاريخ 23/04/07 عن غرفة الجنايات الخاصة بالأحداث بنفس المحكمة في ملف قدد 23/05/50 والقرار عدد 364 الصادر بتاريخ 2006/04/17 في الملف عدد 22/05/340 وقد أيد هذا القرار جزئيا بمقتضاها قرار صدر بتاريخ 2006/07/19 في الملف عدد 26/06/600.)

ويمكن اعتبار ما ذهبت إليه اجتهادا يحسب لها حين اعتبرت الشباك الأوتوماتيكي نظاما المعالجة الآلية للمعطيات وأصبح خذا الولوج غير مشروع أي أن طريقة الاحتمال عندما استعملت فيه بكافة بطاقات ائتمان مزورة ورقما سريا لا يعود لمستعمل هذه البطاقة.

ومن صور الاحتيال كذلك ، استخدام بطاقات ائتمان مزورة أو مزيفة للولوج الى الشباك الأوتوماتيكي وسحب مبالغ مالية من أرصدة أصحابها الشرعيين، أو الحصول على مشتريات عبر الأنترنت عن طريق استخدام أرقام سرية مقرصنة لبطاقات ائتمان تخص أصحابها من غير مستعمليها التي تضعها المواقع الإلكترونية شرطا للولوج إلى أجزاء خاصة من أنظمتها المعلوماتية، فإذا ما أدخل الجاني رقما سريا لا يملكه يكون قد احتال على إدارة الموقع الالكتروني لكي يسمح لها الولوج الى موقعها والتسوق عبره وهو ما نستخلصه من قراءة الحكم الصادر عن المحكمة الابتدائية بالرباط بتاريخ 2012/05/10.

وقد اعتبرت المحكمة أن الجريمة المعلوماتية هي الثابتة في حق الظنين وعلى هذا الاساس سن المشرع المغربي مجموعة من المقتضيات التي تعد خرقا للنظام المعلوماتي وعليه لا يمكن متابعة الظنين من أجل فعلين بوصف قانوني

واحد، وهكذا أدانت المحكمة المتهم بجريمة التزييف وتزوير وثائق معلوماتية بغرض إلحاق الضرر بالغير واستعمالها مع العلم بأنها مزورة ومزيفة.

ونود أن نشير في هذا الاطار الى انه قبل سنة 2003 أي سنة صدور القانون رقم 07.03 المتعلق بالمس بنظم المعالجة الآلية للمعطيات ذهبت محكمة الاستئناف بالدار البيضاء في قرارها الصادر بتاريخ 2000/04/07 بشأن القضية التي عرضت عليها والتي تتلخص وقائعها في كون موظف بإدارة الجمارك استعمل رمزه السري للولوج الى قاعدة البيانات مضمنة بجهاز الكومبيوتر بإدارة الجمارك وسجل بها معلومات مخالفة للحقيقة، حيث قضت المحكمة بمتابعته من أجل جنحة التزوير في وثائق إدارية طبقا لمقتضيات الفصلين 360و 361 إدارة الجمارك بمثابة سجل رسمي للإدارة وأن إحداث أي تغيير عن قصد في المعلومات المسجلة فيها وجعلها مخالفة للحقيقة يعتبر تزويرا في وثيقة إدارية.

وللاستيضاح موقف القضاء المغربي من هذا النوع من الجرائم فقد اعتبرت المحكمة الابتدائية بالرباط عرقلة النظام كل ما من شأنه أن يحول دون السير العادي المستمر للنظام، وهو توجه نلمسه من خلال مجموعة من القرارات منها القضية المعروفة فيروس zotob عندما قام المتهمان بإرسال الغير الاخير الى مختلف الانظمة المعلوماتية الخاصة بمختلف المؤسسات والشركات العالمية المتواجدة بأمريكا مما أسفر على عرقلة سير هذه الانظمة وإحداث خلل فيها، وجعلها غير قادرة القيام بوظائفها المعتادة كما كبدها خسائر مالية كبيرة ومهمة حسب ما أكدته الخبرة المنجزة في الموضوع (قرار عدد 721 صدر بتاريخ 2006/09/12 في الملف عدد 22/06/600 عن غرفة الجنايات الابتدائية بمحكمة الاستئناف بالرباط ملحقة حي السلام بسلا.)، وكذا القضية المتعلقة باختراق الموقع الالكتروني لوزارة العدل المغربية حيث قام المتهمون بزرع برنامج يدعى Chelly داخل الموقع وهو ما مكنهم من السيطرة على الموقع الالكتروني المذكور وإيقاف سير عمله عن طرق التحكم في الخادم الرئيسي فيه (حكم عدد 701 صدر بتاريخ 2010/05/17 عن المحكمة الابتدائية بالرباط في ملف جنحي تلبسي.).serveur.

وما يمكن تسجيله بهذا الصدد ، هو أن المحكمة لم توضح عنصر العمد في ما قام به الجناة على خلاف ما ذهب إليه المشرع المغربي في الفصل 607-5 من القانون الجنائي الذي ينص على أن فعل العرقلة أو التعطيل يجب أن يتم عمدا ، لكن قيام الجناة بعرقلة سير أنظمة المعالجة المذكورة عن طريق استهدافها ببرامج تشمل عملها وتجعل الجناة يتحكمون فيها يدل على أن قيامهم العمل كان عن عمد وليس مصادفة أو خطأ وهو ما كان على المحكمة حريصة على توضيح عنصر العمد في جريمة الدخول غير مشروع لنظام المعالجة الآلية للمعطيات وهو ما يستشف من خلال وقائع الحكم الصادر بتاريخ 10 مارس 2016 (حكم يدون عدد ملف رقم 2014/2106/6271 الصادر بتاريخ 10 مارس 2016 عن المحكمة الابتدائية بالرباط.) حيث يستفاد من محضر الشرطة القضائية المنجز في النازلة بتاريخ 2014/07/10 تحت عدد 2176 ج ج /ش ق من قبل شرطة الرباط، أنه بناءا على المسطرة المرجعية عدد 20163 ش .ق المتعلقة بالحصول على تذاكر السفر عبر الطائرة عبر الدخول عن طريق الاحتيال الى نظام المعالجة الآلية للمعطيات تم إيقاف المتهمة ... نظرا لغياب ما يفيد عنصر العمد في الواقعة حيث حللت المحكمة موقفها كما يلي "وحيث إن الجنحة المتابع بها الظنينة أي جنحة

الدخول عن طريق الاختيال هي نوع من الجرائم العمدية وترتكز أساسا على الدخول إلى النظام بسوء نية وعن طريق الاحتيال.

حيث إن الملف خال مما يفيد أن الظنينة نفسها قامت بهذا التصرف بسوء نية أو قامت باستعمال الاحتيال من أجل الدخول الى مجموع أو بعض نظام المعالجة الآلية للمعطيات كما يقتضي فصل المتابعة أعلاه، وحيث إن المحكمة بناءا على ما ذكر أعلاه، وبعد دراستها للقضية واعتبارا لقاعدة أن البراءة هي الأصل اقتنعت بان نسب الظنينة غير ثابت في حقها مما يتعين التصريح بعدم مؤاخذتها."

وما قيل سابقا عن ضرورة توفر عنصر العمد بخصوص الجريمة عرقلة سير النظام، يقال عن تغيير المعطيات المدرجة فيه وباقي الجرائم المنصوص عليها في ذات الفصل الذي جاء فيه ما يلي" يعاقب ... كل من أدخل معطيات في نظام المعالجة الآلية للمعطيات أو أخلفها أو حذفها منه أو غير المعطيات المدرجة فيه أو غير طريقة معالجتها أو طريقة إرسالها عن طريق احتيال.

ويتضح من خلال ما سبق أن الجريمة المعلوماتية فرضت نفسها على المشرع المغربي لما تتسم به من خطورة وخصوصية فكان أن سن مقتضيات زجرية خاصة ملائمة حيث جرم مجموعة من الافعال الماسة بنظم المعالجة الآلية للمعطيات الى جانب مطالب اليوم تنبني استراتيجية مرنة في التشريع في هذا الصنف من الجرائم نظرا لسرعة التطور والانتشار الذي يطبع الجريمة الالكترونية (سليمان، 2017، صفحة 133).

إلا أنه مهما قلنا ومهما سطرنا من قواعد موضوعية تهم الجريمة المعلوماتية فأننا سنصطدم بحواجز نظرا لمحدودية الآليات التقليدية في أداء هذه المهمة حيث إن هذه الاخيرة وجدت من أجل إثبات الجريمة المادية المعلوماتية التي ترتكب في فضاء واقعي ملموس في الوقت الذي نجد أن أهم ما يميز الجريمة المعلوماتية أنها جريمة افتراضية ترتكب في فضاء غير محسوس ناهيك عن طابعها العابر للحدود بفضل الوسائل المعتمدة فيها.

مما يتضح معه الحاجة الى اعتماد قواعد اجرائية خاصة بمواكبة تنسجم ومبادئ العدالة الجنائية في حفظ الامن وعدم الافلات من العقاب.

خاتمة:

ختاما، يمكن القول بأن الجريمة الإلكترونية ظاهرة إجرامية مستجدة تحمل في طياتها العديد من المخاطر وتكلف ضحاياها خسائر جسيمة، إضافة إلى أنها في المقابل نتيجة حتمية للتطور العلمي والتقني الذي شهده عصر المعلوميات، لذا فالتصدي لهذا النمط من الإجرام لا يتحقق باعتماد النصوص التقليدية على اختلافها، بل على المشرع تطوير ترسانته القانونية وعدم الاعتماد على النصوص التي سنها والتي لم تتضمن مجمل الجرائم الإلكترونية، وهو ما جعل النص المطبق محل غموض على الكثير من الأفعال التي يعتبرها الفقه الجنائي جرائم إلكترونية، لاسيما وأن القانون الجنائي محكوم بمبادئ لا مناص منها كمبدأ الشرعية، عدم جواز التفسير الواسع وكذا انعدام القيام.

والأكيد أن هذا الفراغ سيتفيد منه الكثير من مقترفي هذه الجرائم، وسيهدد الحياة الشخصية والمالية للعديد من الأشخاص الذين يتعرضون لاعتداءات أو تهديدات ذات طابع إلكتروني، وتجدر الإشارة إلى أن المشرع المغربي وإن

كان نص على القانون الموضوعي لهذه الجرائم إلا أنه لم يفرد أي مقتضيات قانونية خاصة بالمسطرة المتبعة في مواجهة مجرمي الجرائم الإلكترونية.

وعليه، فلابد من إيلاء الاهتمام بآليات البحث المعتمدة في رصد الجريمة التي تبقى محدودة لاحتواء مظاهر إساءة استخدام المعلوميات، فالقدرة التي تنقل بها المعلومات والآثار المدمرة التي تخلفها الهجمات الواقعة على الأنظمة المعلوماتية يحد من التدخلات الزجرية خاصة على شبكة الأنترنت، مما يقتضي مراجعة قانون المسطرة الجنائية حتى يستجيب لمتطلبات البحث وتفتيش قواعد المعطيات الآلية باستعمال الشبكة، دون أن ننسى أهمية تأهيل الشرطة التقنية وسلطات التحقيق في جمع الأدلة باستعمال التقنيات العلمية، مع وجوب التفكير في تطوير اتعاون العربي والدولي.

قائمة المراجع:

1) **751/2010/19, ق. ع. (2012).مجلة .الرباط, المغرب ،2 منشور بقضاء محكمة الاستئناف عدد.**

2) أحمد البخثي. (2004/2003). استعمال الوسائل الإلكترونية في المعاملات التجارية. رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص. الرباط، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية السويسي، المغرب.

3) الإرهاب، ق. ر ,2003) .ماي 29 .(قانون رقم 03.03 المتعلق بمكافحة الإرهاب . الصادر بتنفيذه هير شريف رقم 1.03.140 . الجريدة الرسمية رقم 112، المغرب.

4) الشوابكة، م. أ .(2004) .الجريمة المعلوماتية .عمان: دار الثقافة.

5) برزجو، ع. ا .(s.d.) .مدى إمكانية تطبيق القانون الجنائي المغربي على جرائم المعلومات. CF مقال .مجلة الأبحاث والدراسات القانونية،، المغرب :دار القلم.

6) عبد الرحيم زروق. (2008). حماية المعطيات من الجرائم المرتكبة عبر الأنترنت. رسالة لنيل دبلوم الدراسات العليا المعمقة في القانون الخاص. وجدة، جامعة محمد الأول، كلية العلوم القانونية والاقتصادية والاجتماعية ، المغرب.

7) عبد السلام بن سليمان. (2017). الاجرام المعلوماتي في التشريع المغربي-دراسة نقدية مقارنة في ضوء أراء الفقه وأحكام القضاء. الرباط: دار الأمان.

8) عبد السلام بنسليمان. (2017). الاجرام المعلوماتي في التشريع المغربي،. الرباط: دار الأمان،.

9) عبد الله دغش العجمي. (2015/2014). المشكلات العملية والقانونية للجرائم الإلكترونية-دراسة مقارنة. بحث لنيل شهادة الماجستير في القانون. جامعة الشرق الأوسط، الاردن.

10) كوثر فرام. (2009/2007). الجريمة المعلوماتية على ضوء العمل القضائي المغربي. بحث نهاية التدريب، . الرباط، المعهد العالي للقضاء، المغرب.

11) محمد الشافعي. (2002). بطاقات الأداء والائتمان بالمغرب. سلسلة البحوث القانونية 5. مراكش، المغرب.

12) محمد محمد شتا. (2001). الحماية الجنائية لبرامج الحاسب الآلي. الإسكندرية: دار الجامعة الجديدة للنشر.

فاعلية برنامج في الارشاد المعرفي -السلوكي في خفض مستوى الإدمان على وسائل التواصل الاجتماعي لدى عينة من طالبات الثانوية العامة في مدارس الكرك

the effectiveness of cognitive-behavioral guidance program in reducing the level of addiction on social media in a sample of high school students in Karak schools

Prof. Ahmed Nile Al Ghurair أ.د. أحمد نايل الغرير
Dr. Ayat al-Kasasbeh د. ايات الكساسبة

ملخص الدراسة:

هدفت الدراسة الحالية الى اعداد برنامج ارشادي يلائم طالبات المرحلة الثانوية وتطبيقه عليهم بهدف التاكد من التخفيف حدة الادمان على استخدامات وسائل التواصل المختلفة وفق المقياس المصمم لهذه الغاية مقياس الادمان على وسائل التواصل (SAS) والمتمتع بدرجات صدق وثبات مناسبة وكذلك التعرف على اثر البرنامج الارشادي المقترح في تخفيف من درجة الادمان على وسائل التواصل، وطبقت الدراسة على عينة طالبات من المرحلة الثانوية في مدرسة تابعة لادارة التعليم في تربية المزار في الكرك / الاردن، حيث تكونت العينة من 20 طالبة تم تقسيمها بالتساوي الى مجوعتين تجريبيه (10) طالبات وضابطة (10) طالبات، وتم تطبيق البرنامج الارشادي لمدة شهر بواقع جلستين اسبوعيا وتم اجراء القياس القبلي والبعدي والتتابعي مقارنة بالقياس القبلي على اكمل واجه، واشارت النتائج الى وجود فروق ذات دلالة احصائية في خفض مستوى الادمان لصالح المجموعة التجريبية مقارنة مع المجموعة الضابطة عند مستوى الدلالة(0,05) مما يؤكد فاعلية واثر البرنامج في احداث تغيير ايجابي ظهر من خلال خفض عدد من سلوكيات واضطرابات الطالبات عينة الدراسة على درجات فقرات مقياس الادمان بشكل واضح من خلال الفحص والاختبارت الاخصائية المستخدمة في نتائج التحليل الاحصائي ذات الموثوقية العالية، وكذلك خلصت النتيجة الى رفع مستوى الوعي والانتباه لدى عينة البحث وانعكاسة على بقية سلوك الطالبات الاخريات من خلال الملاحظة والتقارير الذاتية ، وهذا الامر يؤكد مدى اهمية البرامج والخدمات الارشادية والعلاجية النفسية في مدارس الاناث في كافة المراحل في خفض مستوى الادمان للمستخمين لوسائل التواصل المختلفة على الانترنت وفي مجتمعاتنا لتلافي اضرارها.

Abstract:

The current study aimed to prepare a guidance program suitable for high school students and apply it to them in order to ensure the reduction of addiction to the uses of different means of communication according to the measure designed to this end the Scale addiction to the means of communication (SAS) and has degrees of sincerity and stability Suitable as well as recognizing the impact of the proposed guidance program in reducing the degree of addiction to communication, and applied the study to a sample of female students from the secondary level in a school under the department of education in the education of the almazar in Karak / Jordan, where the sample consisted of 20 female students divided equally into Two experimental groups (10) female students and a female officer (10) female students, and the extension program was implemented for a month by two sessions a week and the tribal, dimensional and sequential measurement was conducted compared to the tribal measurement at the fullest encounter, and the results indicated the existence of differences statistically significant in reducing the level of addiction in favor of The experimental group compared with the control group at the level

of indication (0.05) which confirms the effectiveness and impact of the program in causing positive change appeared by reducing the number of behaviors and disorders of the students sample the study on the grades of the paragraphs of the measure of addiction clearly through the examination and specialized tests Used in the results of the statistical analysis with high reliability, as well as the result to raise the level of awareness and attention in the sample of research and reflect on the rest of the behavior of other students through observation and self-reports, this confirms the importance of programs and services guidance and treatment Psychological in female schools at all stages in reducing the level of addiction to the various means of communication on the Internet and in our societies to avoid damage.

مقدمة:

تعد وسائل التواصل الاجتماعي من أكثر الأدوات التي استحوذت على شبكة الانترنت، وليس سرا أنها تستهلك الكثير من حياة الإنسان، وبالرغم من إيجابيات استخدامها ولما تشكله من حالة في زيادة مستوى الوعي الفكري والثقافي، إلا أنها قد تشكل تهديدا وخطرا على العديد من النواحي العقلية والنفسية والجسدية للإنسان.

وازداد الاهتمام بدراسة إدمان وسائل التواصل كظاهرة انتشرت بين الأفراد في المجتمعات المختلفة وربما يرجع ذلك إلى ما لهذه الظاهرة من آثار متعددة نفسية واجتماعية وصحية تؤثر على الأشخاص المستخدمين لها، فمع استمرار قضاء مستخدمي وسائل التواصل المزيد من الوقت على الخط المباشر من الطبيعي أنهم يخصصون وقتاً أقل للنشاطات الأخرى والأشخاص الآخرين في حياتهم مع عدم إغفال الدور الكبير الذي تقوم به، حيث تنقل كميات هائلة من المعلومات بين أبناء الجنس البشري بسرعة مذهلة حيث جعلت العالم قرية كونية صغيرة يتفاعل أهلها مع بعضهم البعض.

وتقدم العديد من الشركات وملفات التعريف والمدونات مثل: فيس بوك Facebook 2006 وتويتر وLinkedIn و2010 twitter وسناب شات snabchat وإنستغرام instgram وغيرها من برامج ، وتطبيقات توفر خدمات للأفراد والجماعات والشركات، حتى أصبحت تستنزف الجميع ماديا ومعنويا وجسديا وخاصة ميزانيات الدول والشركات العالمية، فاستخدام وسائل التواصل العديدة لها فوائدها وإيجابياتها في حياة الافراد والمؤسسات، وفتحت افاقا في التفاعل بين الافراد ووفرت المعلومات والمعارف والخبرات لمستخدميها رغم اثارها السلبية أحيانا نتيجة سوء استخدامها(kyriaki,G&George,k2014)

وكغيرها من المهن تأثرت مهنة الارشاد والخدمات النفسية الى حد كبير بهذه التطورات الهائلة في مجال التكنولوجيا، وخلقت وسائل التواصل المتعددة قضايا جديدة لعمل المهنيين والمستشارين في التوجيه المهني والتربوي والارشاد النفسي والأسري والمدرسي والصحي، وفتحت تلك الوسائل الباب على مصراعيه لفرص عديدة للعمل من مختلف التخصصات لتقديم الخدمات بكافة اشكالها للفئات والمؤسسات في المجتمعات الحديثة ومن مختلف أطراف الكرة الأرضية بشكل سريع ومتقدم، وضمن منهجيات واستراتيجيات علمية حديثة.

وتؤكد جمعية الارشاد الامريكية ACA ,2014 وهي منظمة غير ربحية الى النهوض بعملية الارشاد باعتبارها من المهن التي يمكن تطويرها بسرعة وتقدم من خلال وسائل التواصل المختلفة، وأشار ديفيد كابلان D,Kaplan,2005 قبل ظهور وسائل التواصل الى أهمية الحماية للمستفيدين من الارشاد وتقديم الخدمات بشكل أفضل، سواء من خلال الطرق والأساليب التقليدية او المساعدة باستخدام وسائل التكنولوجيا المختلفة بما فيها وسائل الاتصال الحديثة التي تضمن الحماية للجميع.

وأظهرت نتائج العديد من الدراسات والتقارير العالمية في العام 2018 المتعلقة باستخدام وسائل التواصل الاجتماعي احصائيات ونسب انتشار عالية، وهذا يؤشر الى ان هناك ادمان فعلي على تلك الوسائل مما يشكل خطر واثار نفسية مدمرة على الانسان وخاصة الأطفال وطلبة المدارس حتى سن 18سنة وطلبة الجامعات حتى سن 24 عاما والتي تعد من أكثر الفئات استخداما لوسائل التواصل.

هذا ويعد مفهوم إدمان الإنترنت من المفاهيم النفسية الحديثة نسبيا، حيث ما زال البحث في هذا المجال محدودا (Wellman, 1996; Brenner, 1997)، وقد كانت Young يونج "أول من استخدمت مصطلح" اضطراب إدمان الإنترنت ثم عدلته إلى مصطلح أطلقت عليه استخدام الإنترنت المرضي (Young, 1996)، ويعد استخدام الإنترنت المفرط هو أقرب ما يكون إلى الإدمان حتى لو لم يتطابق مع إدمان المخدرات، فكلاهما يعبر عن تجربة ذاتية ويجمع بينهما تغير المزاج، والانسحاب الاجتماعي، والشعور بالضيق والكدر والوحدة، والتي غالبا ما تظهر أعراضها عند توقف الفرد عن استخدام الإنترنت (شاهين2015).

فقد تم إطلاق Facebook في عام 2004 بحدود استخدام طلاب الجامعات وتحديدا جامعة هارفردHarfard وما لبث ان توسع وانتشر كوسيلة تواصل اجتماعي في العالم حتى وصل عدد المستخدمين النشطين يقدر بنحو 2.2 مليار مستخدم شهريًا و1.4 مليار مستخدم نشط يوميًا في العام 2018 ومقاطع الفيديو والاعلانات في Facebook مرتفعاً حيث يبلغ عدد مشاهدات الفيديوهات حوالي 8 مليارات يوميًا.

إضافة لذلك أصبح كل من يوتيوب youtube,2005 وسيلة اتصال شعبية هامة وبمعدل 1,6 مليار مشاهدة شهريا، وكذلك تويتر Twitter,2006 وسيلة لنشر الاحداث العالمية عبر الرسائل النصية وبنسبة انتشار وصلت عام 2018 الى 1.5 مليار مستخدم، كما وتم إنشاء انستقرام Instagram,2010 بحولي مليار مستخدم شهريا، ويعد تطبيق واتس اب watsup,2009 تطبيق مراسلة فورية ويستخدم من قبل مليار مستخدم حتى العام 2018 وانطلقت شبكة تواصل اجتماعي جوجل Google,2011 كعنصر هام في عالم التواصل ولديها 2 مليار مستخدم حتى عام 2018 مسجل على مستوى العالم.

وتعد النسبة الأكبر لاستخدامات وسائل التواصل السابقة الذكر في الدول الأوروبية وامريكا وكندا حيث تصل نسبة الاستخدام الى أكثر من 95 % من الافراد في العام 2018 والاقل في الشرق الأوسط وبنسبة 40% من الافراد في العام نفس، ليس المهم كم عدد المستخدمين لأي شبكة اجتماعية، ان ما يهمنا حقا هو كم عدد الأشخاص الذين

يمكنك الاتصال بهم بطريقة ملائمة، فإذا كان هناك 2.2 مليار شخص يستخدمون فيس بوك، لكن لا أحد منهم يهتم بالقصص التي تقولها (أو لا يمكنك الوصول إليها) فاذا لا قيمة لهذه الشبكة رغم شهرتها وأهميتها للبعض، لذلك عند التفكير في وضع خطة عبر وسائل التواصل الاجتماعي، لا بد من الاهتمام بما هو يحقق الهدف والعائد من التواصل مع الاخرين.

تشير إحصاءات عالمية صادرة من عدة جهات دولية ان هناك أكثر من ثلاثة مليارات شخص حول العالم يستخدمون مواقع التواصل الاجتماعي، أي ما يعادل 50% من سكان العالم. كما إننايقضون في المتوسط نحو ساعتين إلى أربع ساعات بالمتوسط في تصفح هذه المواقع والتفاعل من خلالها، وذلك وفقا لبعض الدراسات الحديثة،

الأدلة التي اشارت لها العديد من الأبحاث حول تأثير وسائل التواصل الاجتماعي على صحتنا محدودة بعض الشيء، وذلك لأن هذه المواقع تعد حديثة نسبيا في حياتنا، لكن المشكلة ان هناك اثار اجتماعية ونفسية واقتصادية وحتى ثقافية بدت تطفو على السطح بشكل أكثر وضوحا، وتعتمد الدراسات المتوفرة حاليا على بعض التقارير الذاتية واستطلاعات الرأي، والتي يمكن في الغالب أن تنطوي على بعض العيوب الإجرائية، كما إن أغلب هذه الدراسات تركز على موقع فيسبوك على وجه الخصوص

ففي العام 2018 وفي ضوء مراجعة العديد من التقارير والأبحاث وراي الخبراء بان ثمة شعور واضح بالتوتر والضغوط النفسية من مستخدمي وسائل التواصل المختلفة، ففي عام 2015، سعى باحثون بمركز "بيو" للدراسات ببيان ان وسائل التواصل واستخداماتها تزيد من حدة التوتر وفي عام 2014، توصل باحثون في النمسا إلى أن المشاركين في إحدى دراساتهم تحدثوا عن تراجع في الحالة المزاجية ووفقا لباحثين من جامعة كاليفورنيا، تم تقييم المحتوى العاطفي مشاعر القلق والاضطراب التي قد تثيرها مواقع التواصل الاجتماعي، والتي تشمل الشعور بعدم الراحة، ومشكلات النوم، وعدم التركيز.

وأكد باحثون بجامعة "بي بي يو" في رومانيا، والذين أجروا في عام 2016 مراجعة واسعة للعديد من الأبحاث التي تتناول العلاقة بين مواقع التواصل، والشعور بالقلق الاجتماعي والشعور بالاكتئاب بان ثمة صلة بين الاكتئاب وبين استخدام مواقع التواصل الاجتماعي، وأن أعراض الاكتئاب، مثل الحالة المزاجية السيئة، والشعور بعدم قيمة الذات، واليأس، كانت مرتبطة بطبيعة ونوع التفاعل على وسائل التواصل الاجتماعي.

وأشارت استطلاعات راي وعدد من الدراسات الى اختلالات في عادات النوم لدى المستخدمين لوسائل التواصل، وتوصل باحثون بريطانيين وفرنسيين إلى وجود صلات بين استخدام مواقع التواصل الاجتماعي واضطرابات النوم، وإلى أن الضوء الأزرق للشاشات يلعب دورا في ذلك. قد يكون أسوأ وقت

فمواقع التواصل الاجتماعي تتغير بوتيرة أسرع مما يمكن للعلماء مواكبتها، وبالتالي، هناك مجموعات متعددة تحاول دراسة ما يعرف بالسلوكيات المرتبطة باستخدامها، وخلصوا إلى أن إدمان مواقع التواصل الاجتماعي يعد مشكلة صحية عقلية "قد" تتطلب علاجا.

وبرى الباحثان إلى أن الاستخدام المفرط لوسائل التواصل المختلفة له صلة بمشكلات في العلاقات مع الناس، وتراجع التحصيل الدراسي، وقلة الانخراط في مجموعات وأنشطة بعيدا عن الإنترنت.

في دراسة كانت تضم 600 شخص بالغ، قال ثلثهم تقريبا إن وسائل التواصل الاجتماعي تشكل لديهم مشاعر سلبية، وخاصة اليأس، وإن السبب الرئيسي وراء ذلك كان الحسد. وكان ذلك يظهر من خلال مقارنة حياتهم بحياة آخرين، وأن المتسبب الأكبر في ذلك كانت صور السليفي التي يلتقطها الآخرون أثناء الرحلات

وتوصلت دراسة نشرت في المجلة الأمريكية للطب الوقائي العام الماضي، والتي استطلعت آراء 7,000 شخص ممن تتراوح أعمارهم بين 19 و32 عاما، إلى أن الأشخاص الذين يقضون وقتا أكثر على مواقع التواصل الاجتماعي، يصبحون أكثر عرضة مرتين للشكوى من العزلة الاجتماعية، والتي يمكن أن تتضمن نقصا في الشعور بالانتماء الاجتماعي، وتراجعا في التواصل مع الآخرين، وفي الانخراط في علاقات اجتماعية أخرى.

الأدلة تشير إلى أن مواقع التواصل الاجتماعي تؤثر على الناس بأشكال مختلفة، وفقا لظروفهم المسبقة، وسمات الشخصية لديهم. والوقت الذي يقضونه عليها، وأن هناك ارتباط وثيق بين حالات الادمان على وسائل التواصل الاجتماعي وبرامج الارشاد والعلاج النفسي المختلفة.

الإطار النظري: الارشاد والعلاج السلوكي المعرفي

واضع نظرية العلاج السلوكي المعرفي (Cognitive Behavior Modification) هو دونالد هربرت ميكينبوم Meichenbaum، وقد كتب مجموعة من المراجع حول الإرشاد والعلاج السلوكي المعرفي ، وكذلك طريقته التي اشتهر بها : التحصين ضد الضغوط النفسيةStress Inoculation ويؤكد ميكينبوم على الاتجاه المعرفي – السلوكي كما عند البيرت أيلليس وآرون بيك وغيرهما، حيث أشار بأن عملية التعلم لا يمكن أن تنحصر في مثير واستجابة كما ترى تلك النظرية السلوكية، بل رأى أنه إذا أردنا تغيير سلوك فرد ما فلا بد أن يتضمن ذلك معتقداته ومشاعره وأفكاره، على أن العنونة والتسميات واللغة والعمليات العقلية العليا لها دور رئيس في عملية التعلم، ويشير هذا الاتجاه المعرفي إلى: أ . إمكانية حدوث استجابات مختلفة لنفس المثير.ب . استجابات متشابهة لمثيرات مختلفة.

مما يشير إلى أن هنالك عوامل أخرى غير المثير والاستجابة تلعب دورا في عملية التعلم وهي: التفكير، والإدراك، والبناءات المعرفية، وحديث الفرد الداخلي مع نفسه، وكيف يعزو الأشياء وكلها تتدخل في عملية التعلم وتتوسط بين المثير والاستجابة، ولها دور في التأثير على سلوك الفرد، لذلك مفيد معرفة ما يدور في تفكير الفرد، وكيف يدرك الموقف؟ وما هو مفهومه عنه.

افتراضات النظرية ومفاهيمها:

انطلق ميكينبوم من الفرضية التي تقول: "بأن الأشياء التي يقولها الناس لأنفسهم Verbal Libations تلعب دورا في تحديد السلوكيات التي سيقومون بها، وأن السلوك يتأثر بنشاطات عديدة يقوم بها الأفراد تعمم بواسطة الأبنية المعرفية المختلفة. إن الحديث الداخلي أو المحادثة الداخلية، يخلق الدافعية عند الفرد ويساعده على تصنيف مهاراته، وتوجيه تفكيره للقيام بالمهارة المطلوبة. ويرى ميكينبوم بأن تعديل السلوك يمر بطريق متسلسل في الحدوث، يبدأ بالحوار الداخلي والبناء المعرفي والسلوك الناتج. إن الاتجاه المعرفي يركز على كيفية تقييم الفرد لسبب انفعاله وإلى طريقة عزوه لسبب هذا الانفعال، هل هو سببه أم هل هم الآخرون؟ ويرى ميكينبوم بأن هناك هدفا من وراء تغيير الفرد لحواره الداخلي. ويجب تحديد حاجة الفرد للشيء الذي يريد أن يحققه، والشيء الذي يرغب في إحداثه في البيئة، وكيف يقيم المثيرات، ولأي شيء يعزى أسباب سلوكه وتوقعاته عن قدراته الخاصة في معالجة الموقف الضاغط.

إن إدراك الفرد يؤثر على فسيولوجيته ومزاجه. ويرى ميكينبوم أن الانفعال الفسيولوجي بحد ذاته ليس هو المعيق الذي يقف في وجه تكيف الفرد، ولكن ما يقوله الفرد لنفسه حول المثير وهو الذي يحدد انفعالاته الحالية. ويرى ميكينبوم بأن حدوث تفاعل بين الحديث الداخلي عند الفرد وبناءاته المعرفية هو السبب المباشر في عملية تغير سلوك الفرد، كما يرى بأن عملية التغيير تتطلب أن يقوم الفرد بعملية الامتصاص، أي أن يمتص الفرد سلوكا بديلا جديدا بدلا من السلوك القديم، وأن يقوم بعملية التكامل بمعنى أن يبقي الفرد بعض بناءاته المعرفية القديمة إلى جانب حدوث بناءات معرفية جديدة لديه. ويشير ميكينبوم بأن البناء المعرفي Cognitive Structure يحدد طبيعة الحوار الداخلي، والحوار الداخلي هذا يغير في البناء المعرفي بطريقة يسميها ميكينبوم بالدائرة الخيرة Virtuous Cycle ، إن على المرشد أن يعرف المحتويات الإدراكية التي تمنع حدوث سلوك تكيفي جديد عند المسترشد وما هو الحوار الداخلي الذي فشل الفرد في أن يقوله لنفسه، ويجب على المرشد أن يعرف حجم ومدى المشكلة، وما هي توقعات المسترشد من الإرشاد، وأن يسجل المرشد أفكاره – المسترشد- ومشاعره قبل وأثناء وبعد مرور المسترشد بالمشكلة التي يواجهها.

أساليب وأنماط الإرشاد السلوكي المعرفي:

1. **إشراط إبدال القلق** :Anxiety-Relief Conditioningهذا التكتيك يتمثل في اقتران المثير المنفر مع تعبير الفرد وحديثه الداخلي مع نفسه ، كأن يقول: اهدأ واسترخ.

2. **أسلوب تقليل الحساسية** :Systematic desensitizationهذا الأسلوب مأخوذ من نظرية ولبي الكف بالنقيض .Reciprocal inhibitionويطلب المرشد من المسترشد أن يكتب هرما بالأشياء التي تخيفه ويطلب منه أن يبدأها من الأقل إخافة إلى الأكثر إخافة، وبعد أن يكون المرشد قد وضعه في حالة استرخاء.

3. **النمذجة** modelingهي طريقة يحصل فيها المسترشد على معلومات من الشخص الأنموذج، ويحولها إلى صور ومفاهيم معرفية ضمنية، وإلى حوار داخلي عنده ليعبر عنها بسلوك خارجي، وهو تقليد الأنموذج، ويعطي معلومات وأوامر لتوجيه المسترشد ليقوم بالعمل المطلوب منه.

4.**الإشراط المنفر** :Aversive Conditioningومثال ذلك تعريض الشخص المتبول إلى لسعة كهربائية لتنفره من عملية التبول. وعندها يقترن ويرتبط التبول بالعقاب، وهو الصدمة الكهربائية مع تكرار عبارات: "أن التبول شيء غير محبب"، "أنا لا أحب أن أكون غير محبوب."

إجراءات أو عمليات الإرشاد :Counseling Process تتضمن عملية الإرشاد ثلاث مراحل تتمثل في:

1.**المرحلة الأولى . مراقبة الذات أو الملاحظة الذاتية** Self-Observation

يقول ميكينبوم:" الفرد في فترة ما قبل الإرشاد أو العلاج يكون عنده حوارا داخليا سلبيا مع ذاته، وكذلك تكون خيالاته وتصوراته سلبية، أما أثناء عملية الإرشاد ومن خلال الاطلاع على أفكار المسترشد ومشاعره وانفعالاته الجسمية وسلوكياته الاجتماعية وتفسيرها تتكون عند المسترشد بناءات معرفية جديدة New Cognitive Structures ، الأمر الذي يجعل نظرته تختلف عما كانت عليه قبل الإرشاد.

2. **المرحلة الثانية . السلوكيات والأفكار غير المتكافئة** :Incompatible Thoughts and Behaviors في هذه المرحلة تكون عملية المراقبة الذاتية عند المسترشد قد تكونت وأحدثت حوارا داخليا عنده. إن ما يقوله الفرد لنفسه، أي حديثه الداخلي الجديد لا يتناسب مع حديثه السابق المسئول عن سلوكياته القديمة. إن هذا الحديث الجديد يؤثر في الأبنية المعرفية لدى المسترشد، الأمر الذي يجعل المسترشد يقوم بتنظيم خبراته حول المفهوم الجديد الذي اكتسبه، وجعله أكثر تكيفا. وهنا يستطيع المسترشد أن يتجنب السلوكيات المناسبة وفقا للأفكار الجديدة.

3. **المرحلة الثالثة . المعرفة المرتبطة بالتغيير**:Cognition concerning Changeوتتعلق هذه المرحلة بتأدية المسترشد لمهمات تكيفية جديدة خلال الحياة اليومية، والحوار مع المسترشد ذاته حول نتائج هذه الأعمال. ويشير ميكينبوم بأنه ليس المهم أن يركز المسترشد لنفسه حول السلوكيات المتغيرة التي تعلمها وعلى نتائجها التي سوف تؤثر على ثبات وتعميم عملية التغيير في السلوك. إن ما يقوله المسترشد لنفسه بعد عملية الإرشاد شيء هام وأساسي، وإن عملية الإرشاد تشتمل على تعلم مهارات سلوكية جديدة، وحوارات داخلية جديدة وأبنية معرفية جديدة. إن على المرشد أن يهتم بالعمليات الأساسية الثلاثي: البناءات المعرفية. والحوار الداخل والسلوكيات الناتجة عن ذلك.

وعليه، فإن عملية الإرشاد تبدأ بتحديد السلوك القديم المراد تغييره. والحوار السالب المتعلق به، وتحاول استبداله بحوار داخلي جديد متكيف ينتج سلوكا متكيفا يؤثر في تكوين بناءات معرفية جديدة لدى الفرد بدلا من القديمة، ومن ثم إحداث السلوك المرغوب، وتعميمه ومحاولة تثبيته. والتدريب على مقاومة القلق والتوتر، أو التدريب على التحصين ضد الضغوطStress Inoculation Training من خلال الخطوات التالية:

1. **مرحلة الكشف عن القلق:** وهنا يجعل المرشد المسترشد على إدراك مشكلته بطريقة عقلانية. إن القلق يرفع من مستوى الانفعال الجسدي، مثل: خفقان القلب، وسرعة التنفس، وتعرق اليدين. ويكون لديه مجموعة من الأفكار المثيرة للتوتر، ولديه أفكارا مخيفة، كالرغبة في الهرب من الخجل. ويهدف الإرشاد إلى مساعدة المسترشد على السيطرة على انفعالاته الجسدية، وتغيير الكلمات التي يقولها لنفسه حول المشكلة.

2. **مرحلة التدريب:** حيث يقوم المرشد بتعليم المسترشد أساليب التكيف مع المشكلة والتوتر، وذلك بمعرفة مخاوفه، والمواقف التي تؤدي إلى توتره، وطرق التخلص منها، وتعلم الاسترخاء العضلي. أما طريقة التكيف المعرفي فتكون بأن يقول المسترشد: أنه يستطيع أن يضع خطة للتعامل مع الوضع، وأن يسترخي، وأنه هو المسيطر على الوضع، وأن يتوقف إذا شعر بالخوف، ثم يقول لنفسه: لقد نجحت.
3. مرحلة التطبيق: عندما ينجح المسترشد في التدريبات السابقة يُعرّض المسترشد لمواقف تثير توتره، أو مواقف مؤلمة. ويكون المرشد قد علم المسترشد كيفية التعامل مع تلك المثيرات.

عندما ينجح المسترشد في التدريبات السابقة يُعرّض المسترشد لمواقف تثير توتره، أو مواقف مؤلمة. ويكون المرشد قد علم المسترشد كيفية التعامل مع تلك المثيرات. وفيما يلي بعض التصورات حول الجوانب المعرفية لدى المسترشدين:

1. العمليات المعرفية باعتبارها أنظمة تفكير غير عقلاني :يدخل في هذا التصور ذلك النموذج الذي وصفه (ألبرت إليس) الذي يرى أن الأفكار غير العقلانية، هي التي تؤدي إلى الاضطراب السلوكي والاضطراب الانفعالي.
2. العمليات المعرفية باعتبارها أنماط تفكير خاطئ :ويدخل في هذه المجموعة ذلك النموذج الذي قدمه (وآرون بيك) الذي يركز على أنماط التفكير المشوه، أو المنحرف الذي يتبناه المسترشد أو المريض. وتشتمل التحريفات على استنتاجات خاطئة لا يقوم عليها دليل، وكذلك على مبالغات في أهمية الأحداث ودلالتها، أو خلل معرفي، أو نقص اعتبار عنصر هام في الموقف، أو الاستدلال المنقسم، أو رؤية الأشياء على أنها أبيض وأسود، خير أو شر، صحيح أو خطأ، دون وجود نقطة وسط، وكذلك المبالغة في التعميم من حادث مفرد، ويُدرب المسترشدون على التعرف على هذه التحريفات من خلال الأساليب السلوكية، واستخدام الدلالات اللفظية.
3. الجوانب المعرفية كأدلة على القدرة على حل المشكلات ومهارات التعامل :اقترح دي زوريلا وجولد فرايد وغيرهم، التركيز على التعرف على غياب مهارات تكيفية ومعرفية معينة، وعلى تعليم المسترشدين مهارات حل المشكلات عن طريق التعرف على المشكلة، وتوليد البدائل الخاصة بالحلول. واختيار واحد من هذه الحلول، ثم اختبار كفاءة هذا الحل. ويركز معالجون آخرون ومن بينهم ميكينبوم على مهارات المواجهة. وفي أسلوب حل المشكلات فإن المسترشدين يتعلمون كيف يواجهون ويحلون مشكلة في مواقف مستقبلية، بينما في مهارات المواجهة فإنهم يتعلمون في موقف أزمة، أو موقف مشكلة حقيقي.

مشكلة الدراسة:

في ضوء مراجعة شاملة للأدب النظري ونظريات علم النفس بما فيها نظرية (الارشاد المعرفي السلوكي) والدراسات السابقة في مجالات الشبكة العنكبوتية ومواقع التواصل الاجتماعي، ظهر للباحثان بان ثمة مشكلة يراها العلماء وتشكوا منها الاسر والمربين، وان الفئة العمرية من الطفولة 6 سنوات الى سن الشباب عي من اكثر الفئات استخداما لوسائل الاتصال وان فئة الطلبة امتدادا من المرحلة المتوسطة وحتى نهاية الجامعة هم الأكثر استخداما لوسائل التواصل الاجتماعي ويظهر عليهم اعراض الإدمان على الفيس بوك ويوتيوب وتويتر وغيرها مما يشكل لديهم العديد من المشكلات النفسية والسلوكية والاجتماعية والمادية كالتوتر والاكتئاب والقلق والعزلة والخوف واضرابات النوم والاضطرابات الاسرية

والعنف والعصبية وغيرها من المشكلات التي اشارت اليها الاستطلاعات والدراسات المسحية والوصفية لواقع استخدام وسائل التواصل.

ولندرة الدراسات التجريبية والارشادية في حدود اطلاع الباحثين على ما سبق من دراسات تم ملاحظة ندرة البرامج الارشادية التي تحد من الإدمان على وسائل التواصل المختلفة ، إضافة الى الطلب المتزايد من مختلف الفئات العمرية التي تبحث عن برامج ارشادية وحلول لمشكلة ادمان استخدام وسائل التواصل الاجتماعي والبحث عن الاستشارة النفسية للتخلص من التوتر والقلق ، كل ذلك وغيرة ، شكل مشكلة قابلة للبحث ولقناعة الباحثان التامة وكون عملهم في مجال الارشاد النفسي وقربهم من الحالات والمتمثل في طالبات وطلاب المرحلة الثانوية والتي تستخدم وسائل التواصل الاجتماعي وتلقيهم للكثير من الاستشارات النفسية والسلوكية الناتجة عن استخدام تلك الوسائل فانه بات من الضروري التأكيد على وجود المشكلة، والتي يمكن صياغتها كمشكلة بحثية على النحو التالي: التعرف على فاعلية برنامج في الارشاد المعرفي السلوكي في خفض مستوى التوتر لدى عينة من طالبات الثانوية العامة في محافظة الكرك ممن يعانون من ادمان على وسائل التواصل الاجتماعي. وتتمثل المشكلة في التساؤل الرئيس التالي: ما فاعلية الارشاد المعرفي -السلوكي في خفض مستوى الإدمان على وسائل التواصل الاجتماعي لدى عينة من طالبات الثانوية العامة في مدارس الكرك؟

فرضيات الدراسة:

في ضوء مما سبق من اطر نظرية ومشكلة الدراسة فقد تم صياغة فرضيات الدراسة على النحو التالي:

1. توجد فروق ذات دلالة إحصائية بين متوسطات درجات افراد المجموعة التجريبية في القياسين القبلي والبعدي على مقياس الإدمان على وسائل التواصل.
2. لا توجد فروق ذات دلالة إحصائية بين متوسطات درجات افراد المجموعة الضابطة في القياسين القبلي والبعدي على مقياس الإدمان على وسائل التواصل.
3. توجد فروق ذات دلالة إحصائية بين متوسطات درجات افراد المجموعة التجريبية والضابطة في القياس القبلي والبعدي على مقياس الإدمان على وسائل التواصل.
4. توجد فروق ذات دلالة إحصائية عند مستو دلالة (0,05) بين متوسطات درجات افراد المجموعة التجريبية في القياسين القبلي والتتابعي على مقياس الإدمان على وسائل التواصل.
5. تظهر فاعلية البرنامج الارشادي المطبق في خفض الإدمان على وساءل التواصل الاجتماعي

أهمية الدراسة:

- **الأهمية النظرية:**

1. إلقاء الضوء على أهمية برامج الإرشاد المعرفي السلوكي من خلال التدخل المبكر وتأثيراته الإيجابية على خفض الإدمان على وسائل التواصل الاجتماعي.

2. إلقاء الضوء على الأسباب الحقيقية التي تؤدي إلى ظهور الإدمان على وسائل التواصل وما ينجم عنه من مشكلات نفسية وسلوكية واجتماعية ومادية.

3. يرغب الباحث في أن تكون الدراسة الحالية نواة لإجراء مزيداً من الدراسات المستقبلية حول فاعلية البرامج الإرشادية المعرفية السلوكية في خفض الإدمان على وسائل التواصل في بيئات ومدارس مختلفة.

- **الأهمية التطبيقية:**

1. يمكن أن تسهم نتائج الدراسة في مساعدة الطالبات والطلاب على التعامل باتزان مع وسائل التواصل الاجتماعي

2. يمكن أن تسهم نتائج الدراسة في مساعدة المرشدين في المدارس في التعامل بصورة واضحة مع مشكلة الإدمان على وسائل التواصل الاجتماعي.

3. يمكن أن تسهم نتائج الدراسة في تصميم برنامج إرشادي معرفي سلوكي مبكر لتوجيه وإرشاد الطالبات في مختلف الأعمار للحد من الإدمان والتعامل الإيجابي مع وسائل التواصل الاجتماعي.

مصطلحات الدراسة:

- **برنامج إرشادي** عملية إجرائية يتم فيها مساعدة المسترشدين على التخلص من مشكلاتهم (نوري، 2011، 256).

- **برنامج معرفي سلوكي** يعرفه الباحثان إجرائياً البرنامج المعرفي والسلوكي في الدراسة الحالية بأنه " برنامج مخطط ومنظم في ضوء مجموعة من الأسس العلمية والفنيات والاساليب الارشادية يهدف إلى تقديم خدمات إرشادية قائمة على تنمية الاتجاهات وزيادة مستوى الوعي لدى الطالبات المدمنات على وسائل التواصل الاجتماعي.

- **التوتر** فقدان القدرة على مواجهة الصعوبات والمواقف التي تواجه الفرد خلال حياته اليومية بسبب قدراته المحدودة سواء تلك الموروثة أم المكتسبة والمتعلقة بالناحية النفسية أو الاجتماعية أو العضوية أو العقلية أو الجسدية. (taylor et al, 2013, p45).

يعرفه الباحث إجرائياً: عدم قدرة الطالبات المدمنات على وسائل التواصل على تحقيق الثبات الانفعالي أثناء استخدامهن لها ويتضمن أثارا من التوتر الفسيولوجي يؤثر على وظائف الجسم وأثر نفسي يؤثر على الحالة النفسية لهم ويسبب الأذى والألم النفسي لهم وأثرا اجتماعي كالعزلة والوحدة وأثرا اقتصادي كالتبذير للأموال

- **الإدمان:** يعرف باللغة الإنجليزية بمصطلح(Addiction) ، ويطلق عليه أيضاً مسمى التعود، وهو عبارةٌ عن حالة نفسية، وسلوكية تؤثر على الإنسان، وتجعله يرغب في القيام بشيء ما من أجل تحقيق الراحة النفسية.

ويعرف الباحثان **ادمان وسائل التواصلة** Social maidia addiction بأنه الاستخدام المفرط والبقاء أطول فترة على وسائل التواصل، ويعرف اجرائيا بالدرجة التي يحصل عليها المفحوص على مقياس الإدمان SAS المستخدم في الدراسة الحالية.

- **وسائل التواصل الاجتماعي**: عبارة عن تطبيقات تكنولوجية حديثة تعتمد على الويب من أجل التواصل والتفاعل بين البشر عن طريق الرسائل الصوتية المسموعة، والرسائل المكتوبة، والرسائل المرئية، وتعمل هذه الوسائل على بناء وتفعيل المجتمعات الحيّة في بقاع العالم، ومشاركة اهتماماتهم وأنشطتهم بواسطة هذه التطبيقات **كالفيس** بوك وتوتر وواتس اب وغيرها.

حدود الدراسة:

- الحدود الموضوعية: سوف يركز موضوع الدراسة على التحقق من فاعلية برنامج إرشاد معرفي سلوكي في خفض الادمان على وسائل التواص الاجتماعي
- الحدود المكانية: سوف يتم تطبيق الدراسة على عينة من طالبات الثانوي في مدارس الكرك.
- الحدود الزمانية: سوف يتم تطبيق الدراسة في العام (2019).

الدراسات السابقة:

- فرح على فرح أو نورالدين، هويدا (2017) هدفت هذه الدراسة إلى التعرف على أثر تطبيق برنامج الإرشاد الجمعي المعرفي السلوكي في تحسين الذكاء الوجداني لدى طالبات المرحلة الثانوية بولاية الخرطوم، ولتحقيق هذه الهدف تم تصميم برنامج إرشادي اعتماداً على خمس مهارات للذكاء الوجداني، وهي "مهارة إدارة الانفعال، مهارة الوعي بالذات، مهارة التعامل مع الآخرين، مهارة تأجيل الاندفاع ومهارة تحسين المزاج". وتم اختيار عينة البحث بالطريقة القصدية وتكون مجتمع البحث الأصلي من(160) طالبة اختارت الباحثة(30) طالبة كمجموعة تجريبية للبحث وهم الآتي انحصرت درجاتهن في الإرباعين الأول. حسب التحليل الإحصائي لدرجات المقياس. وتم استخدام أداتين هما: مقياس الذكاء الوجداني وبرنامج الارشاد الجمعي المكون من نشرات إرشادية بطاقات الواجب المنزلي استمارات تقييم. وتلخصت مشكلة الدراسة في السؤال الرئيسي التالي: ما مدى فعالية برنامج الإرشاد الجمعي المعرفي السلوكي في تحسين الذكاء الوجداني لدى طالبات المرحلة الثانوية بولاية الخرطوم؟ وانطلاقاً من التساؤل السابق تختبر الدراسة الفروض التالية: توجد فروق بين القياس القبلي والبعدي لدى المجموعة التجريبية في بُعد إدارة الانفعال لصالح القياس البعدي، كما وجد فروق بين القياس القبلي والبعدي لدى المجموعة التجريبية في بُعد الوعي بالذات لصالح القياس البعدي، اضافة لوجود فروق بين القياس القبلي والبعدي لدى المجموعة التجريبية في بُعد التعامل بالحسنى مع الآخرين لصالح القياس البعدي، كما وتوجد فروق بين القياس القبلي والبعدي لدى المجموعة التجريبية في بُعد اليسر الانفعالي في التفكير لصالح القياس البعدي، كما وتوجد فروق بين القياس القبلي والبعدي لدى المجموعة التجريبية في بُعد الحالة المزاجية لصالح القياس البعدي. واستخدم الباحثين لمعالجة البيانات برنامج الحزمة الإحصائية (SPSS) وتم تحليل البيانات باستخدام التكرار، الانحراف المعياري، تحليل التباين، اختبار مربع إيتا.وكانت أبرز النتائج الدراسة: وجود أثر قوي للبرنامج الإرشادي في زيادة القدرة على إدارة الانفعال لدى أفراد العينة، ووجود أثر قوي للبرنامج الإرشادي في زيادة الوعي بالذات لدى أفراد العينة، وأثر للبرنامج الإرشادي في زيادة القدرة على التواصل مع الآخرين لدى أفراد العينة، وفي زيادة القدرة على اليسر الانفعالي في التفكير لدى أفراد العينة، وفي تحسين الحالة المزاجية لدى أفراد العينة.

- دراسة العبيدي، ناصر ودبيس، سعيد (2017) أثر برنامج ارشادي لخفض درجة ادمان الانترنت لدى طلاب المرحلة الثانوية في الرياض، مشكلة الدراسة: هل يؤدي استخدام البرنامج الإرشادي المقترح إلى خفض درجة الإدمان على الانترنت لدى عينة طلاب المرحلة الثانوية المختارة ممن يوصفون بأنهم مدمنون للانترنت حسب مقياس الإدمان على الانترنت المستخدم في هذه الدراسة؟ أهداف الدراسة: -تصميم برنامج إرشادي ملائم لطلاب المرحلة الثانوية وتطبيقة عليهم بهدف تخفيف درجة الإدمان على الانترنت لديهم وفق مقياس الدراسة. -التعرف على أثر البرنامج الإرشادي المقترح في التخفيف من درجة الإدمان على الانترنت لدى عينة الدراسة. مجتمع وعينة الدراسة: طبقت الدراسة على طلاب المرحلة الثانوية الحكومية النهارية بمدينة الرياض، حيث طبق المقياس على طلاب الصف الثاني والثالث ثانوي في ثانوية العليان بحي الريان لاستخراج المجوعة الضابطة وفي ثانوية الصديق بحي المنار لاستخراج العينة التجريبية وكلاهما تابعتين لمكتب إشراف الروابي التابع الدارة تعليم الرياض للبنين، وقد تكونت العينة الضابطة من (14) طالباً والعينة التجريبية من (14) طالباً ممن حققوا درجات مرتفعه على مقياس إدمان الانترنت المستخدم في الدراسة. منهج الدراسة وأدواتها: تم استخدام المنهج التجريبي والذي يعتمد على مجموعتين متكافئتين مع القياس القبلي والبعدي لهما، وتطبيق البرنامج الإرشادي على المجموعة (التجريبية) وحجبه عن (الضابطة). أهم النتائج: أشارت النتائج إلى وجود فروق داله إحصائيا بين درجات أفراد المجموعة التجريبية في مستوى إدمان الانترنت وأبعاده في القياس القبلي والبعدي لصالح القياس البعدي، كما أظهرت نتائج الدراسة وجود فروق دالة إحصائيا بين أفراد المجموعة التجريبية وأفراد المجموعة الضابطة في مستوى إدمان الانترنت في أكثر أعراضه في القياس البعدي لصالح أفراد المجموعة التجريبية، وفي ذلك إشارة إلى أثر البرنامج الإرشادي وجدواه في خفض درجة إدمان الانترنت لدى طلاب المرحلة الثانوية في مدينة الرياض. أهم التوصيات: - زيادة إهتمام المرشدين الطلابيين باضطراب إدمان الادمان على الانترنت باعتباره من الاضطرابات السلوكية الحديثة بين الطلاب والاستفادة من الدراسة الحالية وغيرها في مجال التوعية بأضراره وخفض درجة إدمانه لديهم. - إجراء الأبحاث عن الأسباب الاجتماعية والنفسية الدقيقة الدافعة لإدمان الانترنت في المجتمع السعودي.
- دراسة (2017) Vikram Kumar,el al فعاليه العلاج السلوكي المعرفي القائم علي وسائل التواصل الاجتماعي(ICBT) في علاج الاضطرابات النفسانية. وقد تم التحقيق في فعاليه ICBT في علاج وأداره الظروف مثل الاكتئاب، اضطراب القلق المعمم (جاد)، اضطراب الهلع، اضطراب الوسواس القهري (الوسواس القهري)، اضطراب الإجهاد ما بعد الصدمة، اضطراب التكيف، ثنائي القطب اضطراب ، والم المزمن ، والرهاب. كما تم استكشاف دور المركز في علاج الحالات الطبية مثل داء السكري مع الامراض العقلية المرضية. وعلاوة على ذلك، تتناول هذه الدراسة بالتفصيل فعاليه التكلفة وأثرها في المناطق الريفية. أجرينا بحثا شاملا عن الأدب باستخدام PubMed وباحث Google مع عدم وجود قيود على التاريخ. وقد أرسي دور المعهد في معالجه الامراض النفسانية والسيطرة عليها في الأدبيات. من البيانات التي تم تجميعها، نستنتج ان ICBT مفيد في علاج الصحة العقلية والامراض الطبية مع اعتلالات نفسيه. وتبين أيضا انه فعال من حيث التكلفة بالنسبة للمرضي والمجتمع. والمركز أداه محتمله ناشئه عن التقدم التكنولوجي في العصر الحديث ومفيد في البيئات الريفية والحضرية، عبر مختلف اللغات والثقافات، وعلى نطاق عالمي. ومن المحتم

ان تسلط تجارب التحكم العشوائية الأكبر على استخدامها في الممارسة السريرية وفي الوصول إلى السكان الريفيين مزيدا من الضوء على فعاليه هذه الاداه إلى جانب نشر الوعي بين الأطباء ومجتمعات المرضي.

- ياسرة أبو هديرس (2016) فاعلية برنامج معرفي سلوكي في علاج الإدمان على موقع التواصل الاجتماعي الفيس بوك لدى عينة من المراهقات هدفت الدراسة الحالية للتعرف إلى مدى فاعلية برنامج إرشادي جمعي قائم على النظرية المعرفية السلوكية في علاج اضطراب الإدمان على موقع التواصل الاجتماعي "الفيس بوك" لدى عينة من الطالبات، ولتحقيق هذا الهدف قامت الباحثة باستخدام مقياس "الإدمان على الفيس بوك" من إعدادها، كما أعدت الباحثة برنامجا إرشاديا يتكون من خمس عشرة جلسة، اعتمدت في مجملها على مجموعة من فنيات النظرية المعرفية السلوكية، وتكونت عينة الدراسة (28) طالبة اعمارهن بيت16 - 18 سنة، ممن يتعاملن مع موقع التواصل الاجتماعي "الفيس بوك" بطريقة مفرطة، تجعلهن يصنفن كمدمنات على هذا الموقع وفق المقياس المستخدم، وقد تم تقسيم هذه العينة عشوائيا إلى مجموعتين متساويتين هما: المجموعة التجريبية والمجموعة الضابطة، كل مجموعة (14* طالبة، وقد قامت الباحثة وبعد انتهاء البرنامج تم تطبيق الاختبار البعدي، ثم بعد شهرين تقريبا تم تطبيق اختبار المتابعة، وقد أظهرت نتائج وجود فروق ذات دلالة إحصائية عند مستوى 0.05 α ≥ بين متوسط درجات المجموعة التجريبية والمجموعة الضابطة على كل من الاختبار البعدي، وكذلك الاختبار التتابعي في مستوى الإدمان على الفيس بوك لصالح المجموعة التجريبية، حيث أظهرت المجموعة التجريبية انخفاضا دالا إحصائيا في مستوى الإدمان على الفيس بوك مقارنة بالمجموعة الضابطة، مما يشير إلى أن البرنامج الإرشادي المستخدم في هذه الدراسة ذو فاعلية في علاج اضطراب الإدمان على موقع التواصل الاجتماعي "الفيس بوك"، وقد أوصت الباحثة بضرورة الاهتمام بتطبيق هذا البـ ا رمج على عينات مختلفة من الشباب والمـ ا رهقين من الجنسين ممن يعانون من اضطراب الإدمان على هذا الموقع.

- طوبال، فطيم (2016) فعالية برنامج إرشادي سلوكي معرفي في خفض أعراض الضغط النفسي لدى عينة من المراهقين المتمدرسين بالثانوية، استخدمت الباحثة المنهج الشبه التجريبي بتصميم المجموعتين المتكافئتين (ضابطة وتجريبية) باختبار قبلي وبعدي .استخدمت الطالبة الباحثة في تنفيذ الدراسة الحالية الأدوات التالية: مقياس الضغط النفسي، البرنامج الإرشادي السلوكي المعرفي إعداد الباحثة .وتكونت عينة الدراسة من (26) تلميذة من المرحلة الثانوية أعمارهن مآ بين (16-19) سنة بولاية سطي، أسفرت نتائج الدراسة على فعالية البرنامج الإرشادي المقترح في خفض أعراض الضغط النفسي وقدرته على تحقيق الهدف من تصميمه لدى عينة الدراسة .وخلصت النتائج إلى ما يلي :توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0,05)بين متوسط رتب درجات أفراد المجموعة التجريبية قبل وبعد تنفيذ البرنامج الإرشادي على مقياس الضغط النفسي لصالح القياس البعدي ، لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0,05) بين متوسط رتب درجات أفراد المجموعة التجريبية والمجموعة الضابطة في القياسين القبلي والبعدي على مقياس الضغط النفسي، توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (05.0)بين متوسط رتب درجات أفراد المجموعة التجريبية والمجموعة الضابطة في القياس البعدي على مقياس الضغط النفسي لصالح

المجموعة التجريبية، لا توجد فروق ذات دلالة إحصائية عند مستوى الدلالة (0,01) بين متوسط رتب درجات أفراد المجموعة التجريبية في القياسين البعدي و التتابعي على مقياس الضغط النفسي.

- شاهين، محمد أحمد (2015)

هدفت الدراسة الى التحقق من فاعلية برنامج معرفي – سلوكي في خفض الإدمان على الانترنت لدى عينة من الطلبة الجامعيين، وتكومن عيمة الدراسة من 60 طالبا وطالبة منهم (30) في المجموعة تجريبية و(30) في المجموعة ضابطة، ممن كانت درجاتهم في الارباع الأعلى من نتيجة مقياس ادمان الانترنت وبعد إجراء القياس القبلي على المجموعتين تم تطبيق البرنامج الارشادي على المجموعة التجريبية وبواقع اثنا عشرة حلسة على مار ثلاثة شهور وبواقع جلسة واحدة أسبوعيا وبعد الانتهاء من البرنامج تم تظبيك القياس البعدي و بغد شهرين تم تطبيق القياس التتابعي. وقد أظهرت نتائج الدراسة وجود فروق ذات دلالة إحصائية عند مستوى الدلالة (0,05) بين المجموعة التجريبية والمجموعة الضابطة في القياس البعدي على مقياس الإدمان لصالح المجموعة التجريبية، مما يشير إلى فاعلية البرنامج الارشادي في خفض الإدمان على الانترنت لدى افراد عبنة الدراسة المجموعة التجريبية، واظهرت النتائج الى استمرارية أثر البرنامج الى ما بعد القياس التتابعي، مما يؤكد فاعلية مثل هذه البرامج وإنها أداة فعالة لخفض الإدمان على الأنترنت ويمكن تعميمها على مؤسسات التعليم العالي الفلسطيني.

هدفت الدراسة الوصفية الى رصد راي المستشارين وعلماء النفس لفترة زمنية محدودة في العام 2014عن دور وسائل التواصل الاجتماعي آنذاك وتحديد المخاطر الأكثر شيوعا الكامنة من وراء استخدام وسائل التواصل الاجتماعي من قبل المستخدمين واهم المعضلات الأخلاقية المحتملة التي قد تنشأ للمستشارين و علماء النفس الذين يحتضنونهم في ممارستهم وبعض الاعتبارات والقضايا المتعلقة بالتعامل مع وسائل ومدونات ومواقع عبر الإنترنت واظهرت عملية الوصف والمسح ابرز تلك المخاطر والتي تمثلت في محاور رئيسية متضمنة الجوانب التالية: علاقات متعددة، الرؤية والخصوصية، الممارسات الأخلاقية واللاأخلاقية ومناقشة المبادئ والحدود المهنية والكلمات المفتاحية في وسائل التواصل الاجتماعي(الاستشارة ، المخاطر ، الأخلاقيات).

- دراسة الرفاعي (2011) هدفت إلى تحديد فاعلية برنامج إرشادي في نعديل سلوك استخدام الإ نترنت لدى طالبات الملك عبد العزيز بجدة المدمنات للإنترنت، ومن خلال المنهج التجريبي بمجموعتين ضابطة وتجريبية ضمت كل منهما (10) طالبات، أظهرت النتائج وجود فروق دالة إحصائيا لدى أفراد المجموعة التجريبية لصالح التطبيق البعدي، وحدوث انخفاض في مستوى استخدام الإنترنت، مما يشير إلى فاعلية البرنامج الإرشادي، وأن أفراد المجموعة التجريبية قد استفادوا من خلال المهارات التي قدمها البرنامج الإرشادي.كما أشارت النتائج إلى استمرارية أثر البرنامج الإرشادي لدى أفراد المجموعة التجريبية التي حافظت على انخفاض مستوى استخدام الإنترنت كنتيجة لاحتفاظهم بما عرفوه من معلومات وما اكتسبوه من مهارات تطبيقية ساعدتهم في تحسين مهارات تعاملهم مع الإنترنت.

لوحظ من مراجعة الدراسات السابقة محدودبة الدراسات التي تناولت الادمان على وسائل التواصل الاجتماعي المختلفة ، وان توفرت دراسات مماثلة تناولت الادمان على الأنترنت وأهمية الارشاد والبرامج المختلفة في الحد من الادمان على الانترنت مثل دراسة: العبيدي، ناصر ودبيس، سعيد (2017) وkyriaki,G&George,k2014 وكما وركزت الدراسات الاكثر حداثة على فاعلية البرامج الارشادية المختلفة في خفض الادمان على الانترنت بشكل عام كما وركزت بشكل خاص بعض الدراسات على اهمية برنامج الارشاد المعرفي السلوكي على الحد من الادمان على وسائل التواصلالاجتماعي مثل دراسة ياسرة أبو هديرس (2016) والرفاعي (Vikram Kumar,el al,2017)(2011).

إجراءات ومنهجية الدراسة:

يتناول هذا القسم وصفاً لمجتمع الدراسة، والعينة، والأدوات، والإجراءات التي تمّ اتّباعها في تطبيق هذه الدراسة، كما يتناول عرضاً موجزاً للبرنامج الإرشادي، وطريقة التحقق من مناسبته لأغراض الدراسة، بالإضافة إلى عرض المقياس المستخدم (ادمان الانترنت)، وطرق التحقق من صدقه وثباته، وعرضٌ للمعالجة الإحصائية المستخدمة.

- **مجتمع الدراسة:**

تَكوّن مجتمع الدراسة من جميع الطالبات اللواتي يستخدمن الانترنت ومواقع التواصل الاجتماعي في المدرسة، حيث بلغ عدد أفراد مجتمع الدراسة (40) طالبة من المدرسة بالصفوف الثامن والتاسع والعاشر.

- **عينة الدراسة :**

تمّ اختيار عينة الدراسة من الطالبات واللواتي هن من ضمن مجتمع الدراسة، حيث تم الإختيار بعد إجراء عدّة خطوات، وهي:

- بلغ عدد الطالبات (مجتمع الدراسة) حسب العينة الاستطلاعية 40 طالبة.
- تم دعوتهن لحضور محاضرة توعية حول ادمان الانترنت.
- حضر المحاضرة (40) طالبة، وعقدت المحاضرة حول مواقع التواصل الاجتماعي والانترنت في مدرسة بنات ذات راس الثانوية.
- تم عرض فكرة البرنامج عليهن بعد انتهاء المحاضرة، وأعجب منهن (32) طالبة بفكرة البرنامج.
- تم تطبيق المقياس (ادمان الانترنت) على الطالبات الموافقات على المشاركة في البرنامج.
- تم اختيار الطالبات اللواتي حصلن درجات مرتفعة في قياس ادمان الانترنت، فبلغ عدد الطالبات (20) طالبة.
- تم عقد جلسة تحضيرية لطالبات للتعريف بالبرنامج الإرشادي بشكل مفصل، وحضر اللقاء (20) طالبة،
- تم تقسيم الطالبات عشوائيا إلى مجموعتين، تجريبية وضابطة، (10) طالبات في المجموعة التجريبية، و(10) طالبات في المجموعة الضابطة.
- تم التحقق من التكافؤ بين المجموعتين على المقياس.

- **أدوات الدراسة:**

من أجل تحقيق أهداف الدراسة؛ تمّ تطوير مقياس ادمان الانترنت، وبناء برنامج إرشادي، وفيما يلي استعراضاً لأدوات الدراسة:

أولا: مقياس ادمان الانترنت

- تمّ تطوير مقياس ادمان الانترنت لأغراض هذه الدراسة، وذلك من خلال الخطوات التالية:

- مراجعة الأدب النظري، والدراسات السابقة في موضوع ادمان الانترنت

- تكوّن المقياس بصورته الأوّلية من (20) فِقرة، تقيس ادمان الانترنت لدى الطالبات، ولكلّ فِقرة سلّم إجابات ثلاثي، يتكوّن من:

✓ كثيرا تحصل على درجة (3).

✓ أحيانًا تحصل على درجة(2).

✓ قليلا تحصل على درجة (1).

وتعكس الإجابات في حالة الفقرات السلبية، وذلك حسب انطباق محتوى الفقرة على المفحوص.

وللتحقق من مناسبة المقياس تم إجراء صدق وثبات له على النحو التالي:

أولا-صدق وثبات المقياس:

تمّ التحقق من صدق المقياس من خلال:

الصدق الظاهري: تمّ عرض فِقرات مقياس إدمان الانترنت بصورته الأوليّة على (10) محكّمين من أعضاء وطُلب منهم إبداء الرأي ومراجعة فقرات المقياس، من حيث مدى وضوح الفقرات، ومناسبة الفقرات لقياس إدمان الانترنت، وتعديل أو حذف أيّ من الفقرات التي يرون أنّها لا تحقق الهدف من المقياس، وقد تم اعتماد إجماع ثمانية من المحكمين لقبول الفقرات، وذلك بنسبة اتفاق (80%) من المحكّمين، وبناء على أراء المحكمين تم إجراء تعديلات على بعض الفقرات، بينما لم يتم حذف أي فقرة من الفقرات، وبقي المقياس بصورته النهائية مكون من (20) فِقرة، للتحقق من تجانس مقياس الدراسة داخليا، تمّ استخدام طريقة الاتساق الداخلي، وهي إحدى طرق صدق البناء (Construct Validity)، حيث تم إيجاد معامل الارتباط بين الفقرة والدرجة الكلية للمقياس، من خلال العينة الاستطلاعية التي تضمّ (15) طالبة، تم إختيارهن من مجتمع الدراسة ومن خارج عينتها، والجدول رقم (1) يوضّح نتائج ذلك.

جدول رقم(01): قيم معاملات ارتباط الفقرة مع الدرجة الكلية لمقياس ادمان الانترنت

رقم الفقرة	الإرتباط مع الدرجة الكلية
1	0.66**
2	0.70**
3	0.65**
4	0.81**
5	0.76**
6	0.59**
7	0.74**
8	0.71**
9	0.89**
10	0.67**
11	0.60**

12	0.82**
13	0.77**
14	0.83**
15	0.79**
16	0.68**
17	0.74**
18	0.74**
19	0.67**
20	0.80**

دالة إحصائيا عند مستوى دلالة ≤α**(0.01) *دالة إحصائيا عند مستوى دلالة **(α≤0.05)**

يظهر الجدول السابق أن جميع فقرات مقياس ادمان الانترنت ترتبط ارتباطا دالا احصائيا عند مستوى الدلالة (≤α0.01) مع الدرجة الكلية للمقياس، في تراوحت معاملات الارتباط بين (0.89_0.59)، كان ارتباط الفقرة السادسة مع الدرجة الكلية للمقياس (0.59)، بينما الفقرة التاسعة فبلغ (0.89)، وجميع القيم داله احصائيا مما يعني ارتباط الأبعاد بالمقياس، وجميعها مؤشرات مناسبة للحكم على صدق الأداة.

ثبات المقياس:

تم استخلاص مؤشرات ثبات المقياس بإستخدام ثبات الإستقرار (الإختبار وإعادة الإختبار)، حيث تم تطبيق المقياس على العينة الإستطلاعية، وإعادة تطبيقه على نفس العينة بفاصل زمني بلغ أسبوعين، وتم إيجاد معاملات الإرتباط بين التطبيقين، والجدول رقم (2) يبين النتائج:

جدول رقم (02): معاملات ثبات الاختبار وإعادة الاختبار لمقياس إدمان الانترنت

الفقرات	الإختبار-وإعادة الإختبار
1	0.71
2	0.85
3	0.69
4	0.70
5	0.82
6	0.66
7	0.59
8	0.72
9	0.80
10	0.58
11	0.79
12	0.62
13	0.68
14	0.76
15	0.69

16	0.74
17	0.81
18	0.59
19	0.84
20	0.78
الكلي	00.80

تظهر نتائج الجدول (2) أن معاملات ثبات الإختبار وإعادة الاختبار بين التطبيقين لمقياس إدمان الانترنت على القياس الكلي بلغت (00.8)، وللفقرات تراوحت بين (0.58-0.85) مما يؤكد تمتّع مقياس ادمان الانترنت بدرجة مناسبة من الثبات، وتُعَدّ مناسبة لأغراض الدراسة الحالية.

تكافؤ المجموعتين على مقاييس الدراسة:

فحص تكافؤ المجموعتين: تمّ التّحقّق من تكافؤ المجموعتين (التجريبية والضابطة) على مقياس ادمان الانترنت في القياس القبلي قبل تطبيق البرنامج الإرشادي، ومن عدم وجود فروق دالّة إحصائياً بين متوسط درجات أفراد المجموعة التجريبية والضابطة قبل البدء بالمعالجة للتأكد من تكافؤ المجموعات على تلك المقاييس، ذلك بتطبيق اختبار (T-Test) لعيّنتين مستقلتين، لتحقق شرط استخدامه (التوزيع الطبيعي للبيانات، وإفتراض تساوي التباين) .ويوضّح الجدول (3) نتائج المقارنة، من خلال قيمة اختبار (T) لدلالة الفروق بين متوسّط درجات المجموعة التجريبية والمجموعة الضابطة، على مقياسي الدّراسة في القياس القبلي.

جدول رقم (03): نتائج اختبار (T-TEST) لتكافؤ المجموعتين التجريبية والضابطة على مقياس ادمان الانترنت على الاختبار القبلي

المقياس	المجموعة	العدد	المتوسط الحسابي	الانحراف المعياري	درجات الحرية	Tقيمة	Sig
الوالديّة الإيجابيّة	التجريبية	10	10.45	1.05	18	0.64-	0.26
	الضابطة	**10**	**10.81**	**1.12**			

تظهر نتائج الجدول(3) عدم وجود فروق ذات دلالة احصائية عند مستوى دلالة≥ α) 0.05) في مقياس ادمان الانترنت على الدرجة الكلية، مما يدل على وجود تكافؤ بين المجموعتين (التجريبية والضابطة) في القياس القبلي.

نتائج التحليل الإحصائي:

استخدم في الدراسة الحاليّة تصميم المنهج شبه التّجريبي، للوصول إلى النتائج، وحساب التّكرارات والنّسب المئوية، والمتوسّطات الحسابيّة والإنحرافات المعياريّة، وإستخدام إختبار مان وتني وإختبار ويلككسون وبإستخدام رزمة البرامج الإحصائية في تحليل بيانات الدراسة (SPSS).

متغيرات الدراسة:

المتغير المستقل: البرنامج الإرشاد الجمعيّ

المتغيرات التابعة: درجات المفحوصات في مقياس ادمان الانترنت.

إجراءات الدراسة: لغايات اجراءات وتنفيذ الدراسة الحالية تم القيام بما يأتي:

- ✓ مراجعة الأدب السابق، تم بناء البرنامج وتطوير مقاييس الدراسة، والتي تتماشى مع أهدافها.
- ✓ إعتماد مقياس الدراسة بصورته النهائية، بعد إستخراج دلالات صدقه وثباته.
- ✓ توضيح أهداف الدراسة وإجراءاتها، للوصول إلى العينة، وتطبيق البرنامج، وذلك للحصول على الموافقة اولياء امور الطالبات، وتحديد من ترغب بالمشاركة في البرنامج، وكذلك تحديد مكان التدريب وزمانه.
- ✓ توزيع أفراد الدراسة عشوائياً إلى مجموعتين: مجموعة تجريبية تتلقى البرنامج الإرشادي، ومجموعة ضابطة لا تتلقى البرنامج ليتمّ مقارنة نتائجها مع المجموعة التجريبية، بعد الإنتهاء من البرنامج
- ✓ إجراء القياس القبلي والبعدي لأفراد عينة الدراسة على جميع فقرات المقياس، ثمّ إعادة تطبيق المقاييس بعد شهرين لقياس المتابعة للمجموعة التجريبية.

➢ **محتوى البرنامج:**

يتمثل البرنامج فيمايلي: تم اعتماد الرنامج الارشادي المعرفي السلوكي على شكل حقيبة ارشادية، تتضمن مقدمة حول الارشاد النفسي والارشاد المعرفي السلوكي وملخص حول نظرياته واهدافه واهداف البرنامج واليات التعامل في الجلسات مع الطالبات من فئة الادمان على وسائل التواصل المختلفة،اضافة الى محتوى الجلسات الارشادية واجراءاتها ومتطلبات كل جلسة ومراعاة تحقيق اهداف الجلسات وتحقيق الهدف العام من البرنامج الارشادي وصولا الى القناعة بالتخلص من ادمان الطالبات عينة الدراسة على وسائل التواصل المختلفة، والقيام بتطبيق مقياس الادمان بعد الانتهاء من الجلسات ثم العودة الى القياس البعدي بعد فترة زمنية مناسبة.

جلسة (1) افتتاحية وتعارف الترحيب بالمشاركين والتعارف بينهم، وإعطاء فكرة للمشاركين عن البرنامج، وتعريفهم بالإجراءات المتبعة في الجلسات والمهمات المطلوبة منهم، وحثهم على أهمية التعاون لتحقيق الأهداف المرجوة من البرنامج الإرشادي، وأهمية الانتظام في الجلسات والاستعداد للمشاركة، وتحديد مواعيد الجلسات اللاحقة، ومناقشة نموذج عقد الاتفاق وتوقيعه. المحاضرة والمناقشة، والحوار، والنماذج الإرشادية الواجب المنزلي

جلسة (2) إعطاء المعلومات حول وسائل التواصل الاجتماعي واستخداماتها، وتزويد المشاركين بمعلومات عن الإنترنت واستخداماته وإدمان وسائل التواصل بما فيها الانترنت مفهومه وأعراضه وأشكاله وطريقة قياسه ومضارها وخاطرها، والاستخدام الصحي. يقوم المرشد بتقديم المعلومات المناسبة عبر وسيلة عرض مناسبة ومشوقة، ويدير نقاشات ثنائية وجماعية مع المشاركين وفيما بينهم، ويمارس أحياناً مع المشاركين بعض التصوير على النمذجة ولعب الأدوار

جلسة (3) التدريب على مهارات مفهوم الذات إعادة تعارف المشاركين على بعضهم، والتعرف إلى المشكلات التي تعاني منها الطالبات أو أصدقائهم، والتعرف إلى مفهوم الذات وخصائصه وأهميته كمكون رئيس للصحة النفسية. المحاضرة – المناقشة والحوار، المناظرات ولعب الأدوار، أوراق العمل والنماذج الإرشادية الواجب المنزلي.

جلسة (4) مهارات توكيد الذات تطبيق مهارات توكيد الذات التدريب التدعيمي، والتمييز بين السلوك التوكيدي والسلوك غير التوكيدي وسلوك التوتر وضبطه، وعلاقة ذلك بسلوك الاستخدام المفرط للإنترنت. المحاضرة – المناقشة والحوار، المناظرات ولعب الأدوار، أوراق العمل والنماذج الإرشادية الواجب المنزلي.

جلسة (5) التعرف إلى فنيات واستراتيجيات التدريب التوكيدي والتدرب عليها تدريب المشاركين على تطبيق أسلوب توكيد الذات من خلال التدريب التدعيمي. المحاضرة – المناقشة الجماعية والحوار – النماذج الإرشادية– الإقناع بضرورة تغيير الأفكار غير المنطقية – أوراق العمل – الواجب المنزلي. ممارسة تمرين التنفس التدريجي وأسلوب الاسترخاء العضلي التدريجي

جلسة (6) مهارات ضبط الذات وتعديل التفكير تعريف المشاركات بمهارات ضبط الذات، ومهارات ضبط التفكير. وتسعى المرشدة إلى تدريب المشاركات، واكتساب مهارات ضبط الذات وضبط التفكير وتقدم شرحاً حول مهارات ضبط الذات تجاه الاستخدام المفرط لوسائل التواصل، ومهارات تعديل التفكير تجاه الحاجة إلى تلك الوسائل أيضاً. من خلال المحاضرة وإعطاء المعلومات والمناقشات الجماعية، وتوظيف فنية إعادة البناء المعرفي، والتدريب عليها، والواجبات المنزلية، وعبر الأسئلة والنقاش للمشتركة

جلسة (7) استراتيجيات التعامل مع إدمان وسائل التواصل:

- ✓ ممارسة العكس، وتحديد وقت الاستخدام: التعرف إلى استراتيجيتي ممارسة العكس وتحديد وقت الاستخدام من خلال تحديد نمط استخدام كل مشاركه لوسائل التواصل وكيفية كسر هذا الروتين، ومن ثم تحديد عدد الساعات المخصصة أسبوعياً لاستخدام وسائل التواصل للعمل على تقليلها.
- ✓ المحاضرة – المناقشة والحوار -النماذج الإرشادية – أوراق العمل – الواجب المنزلي. وبناء جدول مخفض لإعادة تنظيم وقت الاستخدام الزائد لوسائل التواصل، ومن ثم توزيع ساعات الاستخدام على أيام الأسبوع في أوقات محددة، وتصوير هذه الممارسات عبر مناقشات جماعية، ومن خلال النمذجة ولعب الأدوار في أجواء من الاسترخاء والألفة

جلسة (8) استراتيجيات التعامل مع إدمان وسائل التواصل:

- بطاقات التذكير واستخدام ساعات التوقف) التعرف إلى فنيات واستراتيجيات للتعامل مع إدمان وسائل التواصل هما: بطاقات التذكير، واستخدام ساعات التوقف، وفي مواقف تتعلق بالاستخدام المفرط لوسائل التواصل، ومن ثم تطبيق هذه الفنيات والتدرب على ممارستها. المناقشة والحوار النماذج الإرشادية، وأوراق العمل: للتدريب على فنيات واستراتيجيات للتعامل مع إدمان وسائل التواصل -والواجب المنزلي. ممارسة تمرين التنفس التدريجي ثم أسلوب الاسترخاء والتخيل (قضاء وقت مميز بدون وسائل تواص

جلسة (9) جلسة ختامية تقييم ومراجعة وقياس بعدي.

عرض وتحليل النتائج:

يتضمن هذا الفصل عرضاً لنتائج الدراسة، ومناقشتها في ضوء أسئلتها، والتوصيات المنبثقة عن هذه النتائج.

النتائج المتعلقة بسؤال الدراسة الذي ينص: هل توجد فروق دالة احصائياً عند مستوى الدلالة $\boldsymbol{\alpha} \leq$ 0.05) بين متوسطات أداء المجموعتين التجريبية والضابطة على القياس البعدي لمقياس إدمان الانترنت تعزى للبرنامج الارشادي؟

للإجابة عن السؤال الأول تمّ استخدام اختبار (كلومجروف – سميرنوف) لفحص اعتدالية التوزيع لأفراد عينة الدراسة (ن= 20) على مقياس ادمان الانترنت كما بالجدول (4)

جدول رقم (04): نتائج اختبار اعتدالية التوزيع الإحتمالي لدرجات الطالبات على مقياس ادمان الانترنت باستخدام اختبار (كلومجروف – سميرنوف)

	كلومجروف – سميرنوف		
المجموعة	الاختبار الإحصائي	درجات الحرية	مستوى الدلالة
التجريبية	1.66	9	0.32
الضابطة	1.59	9	0.32

وبناء على نتائج التحليل الواردة في الجدول (4)، والتي أشارت إلى أن استجابات الطالبات (المجموعة التجريبية) على الدرجة الكلية لا تحقق افتراض التوزيع الطبيعي، لذا تم استخدام اختبار" مان ويتني " اللامعلمي.

وعلى الرغم من أن الاختبارات اللامعلمية تتعامل مع رتب المتوسطات فإنه تم حساب المتوسطات الحسابية للتعرف على الفروق الظاهرة بين متوسطات أداء أفراد المجموعتين التجريبية والضابطة.

الجدول رقم (05): المُتوسِّطات الحسابية والانحرافات المعيارية لأداء أفراد المجموعتين في القياس البَعدي على مقياس ادمان الانترنت

الدرجة الكلية		
	المُتوسَّط الحسابي	الانحراف المعياري
المجموعة التجريبيّة	2.99	0.44
المجموعة الضّابطة	1.61	0.44

يَتَّضِح من الجدول (5) وجود فروق ظاهرية بين المجموعتين في الدرجة الكلية، وللتحقُّق من أن الفروق ذات دلالة إحصائيَّة تمَّ استخدام اختبار مان وتني (Mann-Whitney) اللامعلي لتوضيح دلالة واتجاه الفروق بين رتب مُتوسِّطات درجات المجموعة التجريبيّة ورتب مُتوسِّطات درجات المجموعة الضّابطة في القياس البَعدي على مقياس ادمان الانترنت على الدرجة الكلية والجدول (6) يوضح نتائج هذا السؤال:

جدول رقم (06): نتائج اختبار (Mann-Whitney)

للتعرف على دلالة الفروق بين المجموعتين التجريبية والضابطة على مقياس ادمان الانترنت على الاختبار البعدي

المجال	المجموعة	العدد	متوسط الرتب	مجموع الرتب	مان وتني	Z	مستوى الدلالة
الدرجة الكلية	التجريبية	10	9.07	90.7	1.000	-2..605**	0.001
	الضابطة	10	6.58	79.00			

**دالة إحصائيا عند مستوى دلالة ((0.01 ≥α

*دالة إحصائيا عند مستوى دلالة ((0.05 ≥α

تظهر نتائج الجدول (6) وجود فروق ذات دلالة احصائية عند مستوى دلالة(≤ α 0.05) بين متوسطي رتب درجات المجموعتين التجريبية والضابطة على مقياس الوالديّة الإيجابيّة على الاختبار البعدي لصالح المجموعة التجريبية و كانت النتائج كالتالي في الدرجة الكلية(**2..605-) دلالة احصائية عند مستوى دلالة (α ≤ 0.05)،

النتائج المتعلقة بسؤال الدراسة الذي ينص على: هل توجد فروق دالة احصائيا عند مستوى الدلالة ≥ **α**(0.05 بين متوسطات أداء المجموعة التجريبية على القياس البعدي والتتبعي لمقياس ادمان الانترنت تعزى للبرنامج الارشادي؟

تم تطبيق مقياس ادمان الانترنت بعد تنفيذ البرنامج مباشرة وبعد مرور شهر من تنفيذه على أفراد المجموعة التجريبية، وللإجابة عن السؤال المتعلق بذلك التطبيق، تم استخدام اختبار (Wilcoxon Method Pairs Signed test) وهو أحد الاختبارات اللامعلمية الملائمة للكشف عن الفروق بين التطبيقين البعدي والتتبعي في حالة العينات الصغيرة الحجم التي لا تتناسب مع افتراضات الاختبارات المعلمية، والجدول التالي يبين النتائج.

جدول رقم (07): نتائج

اختبار Wilcoxon Method Pairs Signed test لفحص الفروق في التطبيقين البعدي والتتبعي لأفراد المجموعة التجريبية على مقياس ادمان الانترنت

ادمان الانترنت	توزيع الرتب	عدد الرتب	متوسط الرتب	مجموع الرتب	قيمةZ	مستوى الدلالة
الدرجة الكلية	سالبة	5	5.00	33.00	0.31-	0.78
	موجبة	5	6.00	40.00		
	تساوي	0				

تظهر النتائج الواردة في الجدول (7) عدم وجود فروق دالة احصائيا عند مستوى دلالة (α ≥ 0.05) بين التطبيقين البعدي والتتبعي على مقياس ادمان الانترنت، مما يشير إلى استمرار تحسن أداء افراد المجموعة التجريبية بأثر البرنامج الارشادي بعد مرور شهراً على تنفيذه.

وأظهرت النتائج عدم وجود فروق دالة احصائيا بين التطبيقين البعدي والتتبعي على مقياس ادمان الانترنت، مما يشير الى استمرار تحسن أداء أفراد المجموعة التجريبية بأثر البرنامج الارشادي بعد مرور شهراً على تنفيذه.

الاستنتاج والمناقشة:

خلصت النتائج في الدراسة الحالية الى فاعلية البرنامج الإرشادي المعرفي السلوكي في خفض الادمان على وسائل التواصل الاجتماعي لدى أفراد عينة الدراسة التجريبية بعد تطبيق البرنامج ومتابعة الطالبات، وتبين أن هناك فرقا بين متوسطي المجموعتين التجريبية والضابطة على مقياس إدمان الإنترنت .ويمكن تفسير هذه النتيجة في ضوء ما تضمنه البرنامج الإرشادي من أنشطة وممارسات قد ساهمت في تقليل عدد ساعات الاستخدام لوسائل التواصل الاجتماعي، أو خفضت من حدة المشاعر السلبية والأفكار والمعارف غير الإيجابية، التي كانت سببا في اللجوء لتلك الوسائل، وكذلك من خلال استعراض الجلسات الإرشادية التي قدمها البرنامج، إذ نجد أن البرنامج الإرشادي قد تناول أساليب متنوعة للتعامل مع إدمان وسائل التواصل الاجتماعي لدى أفراد المجموعة التجريبية، مثل: مناقشة مفهوم إدمان وسائل التواصل والاستخدام المفرط لها، وآثاره السلبية، المعرفية، النفسية، الاجتماعية وإعادة البناء وآليات التعامل للإستخدام المفرط لها، من خلال تحديد وقت الاستخدام، وممارسة العكس، واستخدام ساعات الوقف، وبطاقات التذكير، وتعديل للأفكار الخاطئة من خلال القوائم الشخصية، والانضمام إلى المجموعات المساندة، ودور الأسرة في ذلك .هذا إضافة إلى ما ظهر من تنفيس للمشاعر من قبل الطالبات في المجموعة التجريبية، وذلك من خلال الأحاديث الذاتية ولعب الدور ومناقشة الواجبات المنزلية التي ارتبطت بالواقع الذي يعيشه الطلبة، وفي أجواء من الاسترخاء الذي أقبلت الطلبات عليه بشغف وتعلمه وممارسته خلال وبعد الجلسات الارشادية.

واتفقت نتائج الدراسة الحالية مع نتائج العديد من الدراسات السابقة مثل دراسة كل من kyriaki,G&George,k2014 وشاهين محمد بالتاكيد على فاعلية البرنامج الارشادي وراي الخبراء في خفض الادمان على وسائل التواصل الاجتماعي والانترنت، وكذلك اتفقت نتائج الدراسة الحالية مع نتائج دراسة Vikram Kumar,el al 2017,) فعاليه العلاج السلوكي المعرفي القائم علي وسائل التواصل الاجتماعي(ICBT) في علاج الاضطرابات النفسانية.

أما بقية الدراسات السابقة فقد تناولت بالوصف والتحليل اهمية البرنامج الارشادي المعرفي السلوكي في خفض الادمان على وسائل التواصل الاجتماعي وتوافقت مع العديد من الفرضيات التي وضعت والتي كانت ذات دلالة احصائية وفروق ايجابية في حال تطبيق البرامج الارشادية ومتابعنها للحالات التي طبقت عليها.

قائمة المراجع:

المراجع باللغة العربية:

1) أبو هديرس، ياسرة. (2016). فاعلية برنامج إرشادي معرفي سلوكي في علاج الإدمان على موقع التواصل الاجتماعي الفيس بوك لدى عينة من المراهقات. رسالة ماجستير، جامعة الأقصى، فلسطين.

2) الرفاعي، صباح. (2011). فاعلية برنامج إرشادي لتعديل سلوك استخدام الإنترنت لدى طالبات جامعة الملك عبد العزيز المدمنات للإنترنت بمدينة جدة. مجلة كلية التربية 4 (21)، 329-372.

3) زين العابدين، فارس. (2014). تأثيرات وسائل الاتصال على الأطفال والمراهقين. المجلة الجزائرية للعلوم، جامعة الجزائر، الجزائر

4) شاهين، محمد أحمد. (2015). فاعلية برنامج معرفي – سلوكي في خفض الإدمان على الانترنت لدى عينة من الطلبة الجامعيين. مجلة الأقصى (سلسلة العلوم الاجتماعية)، 12(02)

5) طوبال، فطيمة. (2016). فعالية برنامج إرشادي سلوكي معرفي في خفض أعراض الضغط النفسي لدى عينة من المراهقين المتمدرسين بالثانوية. أطروحة دكتوراة، جامعة محمد لمين دباغين سطيف-2 ، الجزائر.

6) العبيدي، ناصر، ودبيس، سعيد. (2017). أثر برنامج ارشادي لخفض درجة ادمان الانترنت لدى طلاب المرحلة الثانوية في الرياض، المجلة الدولية المتخصصة، 6(5).

7) فرح، على فرح، ونورالدين، هويدا عباس. (2017). فعالية برنامج إرشاد جمعي سلوكي معرفي في تحسين الذكاء الوجداني لدى عينة من طالبات المرحلة الثانوية بمحلية الخرطوم: جامعة السودان للعلوم والتكنولوجيا. المجلة الدولية المتخصصة، 6 (5)

المراجع باللغة الأجنبية:

8) Kaplan,dievid.(2019). Use of social media in vocational guidance,ACA at;http:www.counseling.org.

9) Kyriaki,G. Giota& George,kleftaras. (2014). Social media and Counseling: Opportunities, Risks and Ethical Considerations,International Journal of Psychological and Behavioral Sciences Vol:R,2014

10) Vikram Kumar , Yasar Sattar , Anan Bseiso , Sara Khan , Ian H. Rutkofsky .(2017) .The Effectiveness of Internet-Based Cognitive Behavioral Therapy in Treatment of Psychiatric Disorders, California Institute of Behavioral Neurosciences and Psychology, Sri ramachandra University.

11) Zine El Abidine, Fares .(2017). Facebook Depression among young adults from Algeria

جريمة الاعتداء على حق الخصوصية عبر الإنترنت في الشريعة الإسلامية والنظام القانوني الأفغاني: "دراسة مقارنة"

The Crime of Privacy Invasion Through Internet on Shariah and Afghan Legislation "a comparative study"

د.أرسلاح ظفري/كلية الشريعة، جامعة غزني/أفغانستان

Dr. Arsalaa Zafari/College of Sharia, Ghazni University/Afghanistan

د.نجيب الله عمري /جامعة بكتيكا/أفغانستان

Dr. Najibullah Omari/ Paktika University/ Afghanistan

ملخص الدراسة:

موضوع "جريمة الاعتداء على حق الخصوصية عبر الإنترنت في الشريعة الإسلامية والنظام القانوني الأفغاني" يرتكز على حق الخصوصية والاعتداء عليه عبر الانترنت وهو: حق الفرد أن يعيش متمتعا باحترام أشياء خاصة يطويها عن غيره في العادة، وذلك بغل يد السلطة العامة، وكذلك الأفراد عن التدخل أو التعرض لهذه الأشياء إلا في الأحوال التي تقتضيها المصلحة العامة، وذلك بإذن الشارع، ويمكن أن يتعدى الشخص على حق الخصوصية لآخر بصور أشهرها، إدخال معلومات وهمية، التجسس الإلكتروني على الحياة الخاصة، سرقة المعلومات الخاصة وتزويرها، التزوير المعلوماتي عن طريق التسلل الإلكتروني إلى البيانات.

الشريعة الإسلامية تمنع هذه الاعتداء وتعتبرها جريمة تعزيرية يفوض تعين جزائها الى رأى الحاكم ، ولهذا جاء قانون العقوبات الأفغاني وصرح أن من اعتدى على حق الخصوصية للغير يحبس مدة لا تزيد على اثنا عشر شهرا .

الكلمات المفتاحية: حق الخصوصية، اعتداء، الشريعة الإسلامية، جريمة الإنترنت، القانون الأفغاني

Abstract:

The article focuses on right to privacy and its violation through internet. It is the right of individual to enjoy with the respect of certain objects that he usually conceals from others, and that belongs to public authority. As well individuals should also refrain from interfering or being exposed to those matters except in cases where public interests required so and it must be with the permission of the legislator. One can violate another's privacy on different ways such as entering fake information, online searching on private life, stealing and falsification of private information.

Shari'ah prohibits this attack and considers it a consolatory crime that authorizes the ruler of its penalty, that's why the afghan penal code stated that whoever attacked the right to privacy of others is imprisoned for a period not exceeding twelve months.

Keywords: Right to privacy, violation, Islamic law, cybercrime and Afghan legeslation

مقدمة:

الحمد لله رب العالمين، والصلاة والسلام على المبعوث رحمة للعالمين سيدنا محمد عليه أفضل الصلاة وأتم التسليم، وعلى آله وأصحابه أجمعين ومن تبعهم بإحسان إلى يوم الدين. وبعد!

عرفت الجريمة منذ القدم بصورتها البدائية البسيطة، كالقيام بعفل أو الامتناع عن فعل يخالف تقاليد وعادات القبيلة أو التعاليم الدينية وما هو سائد من أعراف، ومع التطور أخذت الجريمة صورا جديدة وأبعادا جديدة عن الصور النمطية التي تعرف بها(غلاييي، 2018، ص65) ومن الطرق الجديدة لارتكاب الجرائم الإنترنت، فقد فرضت شبكة الإنترنت، فعلى الرغم من الفوائد العديدة التي لا تحصى للاستفادة من الإنترنت إلا أنه في نفس الوقت قد زادت أساليب الاستخدام لتلك الشبكة بارتكاب بعض الجرائم ومنها جرائم الاعتداء على حق الخصوصية.

هذا ولما لهذا الموضوع من أهمية استعنت بالله تعالى وشرعت بالكتابة فيه مبينا الجرائم الإنترنتية على حق الخصوصية وعقوبتها في الشريعة الإسلامية والقانون الأفغاني. وأسال الله التوفيق والسداد

أهمية الدراسة:

تمكن أهمية البحث في أهمية الموضوع ذاته بوصفه يسلط الضوء على أهم الجرائم المستحدثة والمعاصر، ولا سيما تلك التي ترتبط بشبكلة الإنترنت والتعريف بها لكونها نوعا جديدا من الجرائم لم تألفا المجتمعات من قبل وخاصة في بلدنا أفغانستان منها، فضلا عن ذلك، فإن أهمية البحث تتجلى بكشف النقاب عن أهم أنواع جرائم الإنترنتية والأسباب والدوافع وراء انتشارها وارتكابها، ومن ثم تعريف الجهات الأمنية والقانونية ومن خلفهم المجتمعات الإنسانية بهذا النوع من الجرائم، وكذلك تتبع الأهمية من خلال وضع الآليات والتصورات اللازمة في كيفية معالجة هذه الجرائم والصعوبات التي تحول دون معالجتها بشكل قانوني.

إشكالية الدراسة:

فإن الشبكة الإنترنية أصبحت أداة للربط والاتصال والاسترجاع بين الناس في مختلف أرجاء الأرض، وباتت تشكل أداة ليس للبحث عن المعلومة فحسب، بل و توظيف هذه المعلومة لأغراض الجريمة، ولا سيما الجرائم على حق الخصوصية، وذلك من حيث إساءة استعمال شبكة الإنترنية، والعمل على توظيفها سلبيا وبشكل غير قانوني، لاشباع رغبات النفسية الإنسانية المختلفة، وكل تلك الرغبات الإنسانية غير المشروعة وولدت جرائم جديدة لم تكن مألوفة لدى المجتمع يمكن أن نطلق عليها جريمة الاعتداء على حق الخصوصية عبر الإنترنت، وهذا هو الجزء الأساسي من إشكالية الدراسة. وعلاوة على هذا فإن إشكالية البحث تتمثل في الإجابة عن التساؤلات التالية:

1. ما المقصود بجريمة الاعتداء على حق الخصوصية؟ وهل باتت تمثل ظاهره؟
2. ما هو خصائص جريمة الاعتداء على حق الخصوصية؟
3. ما هي طروق اثبات جريمة الاعتداء على حق الخصوصية؟
4. ما هي عقوبة هذه الجريمة في الشريعة الإسلامية والنظام القانوني الأفغاني؟

أهداف الدراسة:

يروم هذه الدراسة إلى تحقيق الأهداف التالية:

- ✓ التعريف بماهية جريمة الاعتداء على حق الخصوصية.
- ✓ بيان خصائص جريمة الاعتداء على حق الخصوصية.
- ✓ بيان طروق اثبات جريمة الاعتداء على حق الخصوصية في الشريعة الإسلامية والنظام القانوني الأفغاني.

منهج الدراسة:

اتبعت في هذا البحث المنهج الاستقرائي والتحليلي للمقارنة بين الشريعة الاسلامية والقانون الأفغاني.

خطة البحث:

تتكون خطة هذا البحث من مقدمة ومبحثين ونتائج البحث وفهرس لمراجع البحث على النحو التالي:

المبحث الأول: تعريف جريمة الإنترنت وخصائصها

المطلب الأول: تعريف الجريمة الإنترنتية في الشريعة والقانون

المطلب الثاني: خصائص جرائم الإنترنت

المبحث الثاني: جريمة الاعتداءعلى حق الخصوصية وحكمها في الشريعة والقانون الأفغاني

المطلب الأول: تعريف حق الخصوصية

المطلب الثاني: صور التعدي الإكتروني على حق الخصوصية

المطلب الثالث: الوسائل التقنية لحماية حق الخصوصية

المطلب الرابع: حكم الاعتداء على حق الخصوصية في الشريعة الإسلامية

المطلب الخامس: عقوبة الاعتداء على حق الخصوصية في الشريعة الإسلامية والقانون الأفغاني

المبحث الأول: جريمة الإنترنت وخصائصها

المطلب الأول: تعريف الجريمة الإنترنتية في الشريعة والقانون

الفرع الأول: تعريف الانترنت

الانترنت: شبكة عالمية عملاقة تربط الملايين من أجهزة الحاسب الآلي المنتشرة حول العالم ببعضها من أجل تبادل المعلومات، ويتيح هذا الربط الواسع للأجهزة فرصا لا مثيل لها من الإتصال وتبادل المعلومات والتعاون والمشاركة في الموارد الوصول إلى المعلومات، وتحتوي شبكة الإنترنت على كميات هائلة من المعلومات تكاد تغطي كافة مجالات الحياة، ولذلك فهي تعتبر إحدي أهم موارد المعلومات في هذا العصر (السبق، 2033، ص.8).

وتعود أصول كلمة إنترنت إلى الكلمة الإنجليزية Internet وهي منقسمة إلى قسمين الأول وهو Inter يعني البينية وكلمة Net التي تعني شبكة وعليه فتكون الترجمة الحرفية هي الشبكة البينية (سلطان، 2012، ص.7).

وكما يدل اسمها فإن شبكة الإنترنت هي شبكة ما بين عدة شبكات تدار كل منها بمعزل عن الأخريات بشكل غير مركزي ولا تعتمد ايا منها في تشغيلها على الأخريات، كما قد تستخدم في كل منها داخليا تقنيات حاسوبية وشبكية

مختلفة، وما يجمع بينها هو أن هذه الشبكات تتصل فيما بينها عن طريق بوابات تربطها ببروتوكول مشترك قياسي هو بروتوكول إنترنت (التميمي، 2017، ص.4).

الفرع الثاني: تعريف الجريمة الإنترنيتة في الشريعة والقانون الأفغاني

الجريمة في اللغة: "الذنب والإثم يقال أجرم فلان: أذنب واكتسب الإثم"(ابن منظور، 1994، ص. 90).

والجريمة في اصطلاح الفقهاء: "محظورات شرعية زجرالله عنها بحد أو تعزير"(الماوردي،1993، ص.322).

والجريمة في القانون: "كل عمل أو امتناع عن العمل يجرمه (يعتبره النظام القانوني جريمة)، ويقرر له جزاء جنائيا وهو العقوبة توقعة الدولة عن طريق الإجراءات التي رسمها المشرع"(وزارة العدلية، 2019، ص.3).

وتعرف جريمة الإنترنت: "بأنها كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموع به يرتبط بالمعالجة الآلية للبيانات أو نقلها"(صغير، 2013، ص.9).

المطلب الثاني: خصائص جرائم الإنترنت

لجرائم الإنترنت عدة خصائص من أهمها ما يلي:

1.جرائم الإنترنت عابرة للحدود: أعطي انتشار شبكة الإنترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب لمرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان ذلك فإن من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر (العجمي،2014، ص.20).

2. مرتكب الجريمة ذو خبرة في الحاسب الآلي والإنترنت: الخبرة الكبيرة والدراية الفائقة بكل ما يتعلق بالحاسب الآلي وشبكة الإنترنت هي ما تميز مرتكب الجريمة المعلوماتية بشكل عام (الغافري، 2009، ص.39).

ولذلك نجد أن معظم من يرتكبون تلك الجرائم هم من الخبراء في مجال الحاسب الآلي وأن الشرطة تبحث أول ما تبحث عن خبراء الكمبيوتر عند ارتكاب الجرائم.

3.صعوبة الإثبات والاكتشاف: مما يميز جرائم الإنترنت عن الجرائم العادية، صعوبة إثباتها؛ لأنها لا تترك في الغالب أثرا ماديا ظاهرا يمكن ضبطه، فضلا عن التباعد الجغرافي الذي يثير الإشكال، وكأن الجاني يقوم بمهاراته الخاصة بتدمير الدليل بمجرد استعماله.

الفرع الثالث: إثبات جرائم الإنترنت:

قلنا أن جرائم الإنترنت يصعب اكتشافها، و إذا اكتشف يصعب ملاحقتها وضبطها ومرتكبوها يتسمون بالذكاء والسرعة الفائقة في ارتكاب هذه النوعية من الجرائم، كما أن الأدلة التقليدية غير ملائمة لإثبات تلك الجرائم (العبودي،2014، ص.14) ولعل صعوبة إثباتها يرجع إلى ما يلي:

1. أن جرائم الإنترنت لا تترك أثرا لها بعد ارتكابها.
2. صعوبة الاحتفاظ الفني بآثارها إن وجدت.
3. تحتاج خبرة فنية ويصعب على المحقق التقليدي التعامل معها والتحقيق فيها.
4. تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها.
5. تعتمد على قمة الذكاء في ارتكابها.

6. ترتكب في دولة ما ويتحقق الفعل الإجرامي في دولة أخرى.
7. غياب الاعتراف القانوني بطبيعة الأدلة المتعلقة بهذه الجرائم (أنور، 2010، ص.336).

المبحث الثاني: جريمة الاعتداءعلى حق الخصوصية وحكمها في الشريعة والقانون الأفغاني

المطلب الأول: تعريف حق الخصوصية

الحق في اللغة: الوجوب، يقال يحق عليك أن تفعل كذا أي يجب، والحق خلاف الباطل والجمع حقوق وحقاق (ابن منظور، 1994، ص.49).

والخصوصية في اللغة: حالة الخصوص وخصوصية الشيء خاصيته يقال: خصه بالشيء يخصه خصا، وخصوصا، والخصوص نقيض العموم ويستعمل بمعنى لا سيما تقول يعجبني فلان خصوصا علمه وأدبه (ابن منظور، 1994، ص.24).

وبإضافة لفظة(حق) إلى (الخصوصية) يمكن أن نتصور معنى هذه الإضافة من الناحية اللغوية بأنها: حق الشخص في أن ينفرد بأمور لنفسه، أو خاصته، على ألا تتخذ هذه الأشياء صفة العموم (هميم،1981، ص.17).

تعريف حق الخصوصية في الشرع:

لم يستعمل علماء المسلمين في القديم مصطلح حق الخصوصية أو الحياة الخاصة، وعدم استعمال الفقهاء لهذا المصطلح لا يعنى أن الشريعة الإسلامية لم تعترف بهذا النوع من الحق، فقد دخل تحت مفهوم الحق عموما، فالشريعة الإسلامية قد اعترفت بهذا الحق ابتداء وعرفت له تطبيقات عديدة منها حق الشخص في حرمة مسكنه والعيش فيه أمنا من تطفل الآخرين عليه، والنهي عن المسارقة البصرية واقتحام المساكن بالنظر والاطلاع على ما يطويه الفرد عن غيره من أسرار في العادة والنهي عن التجسس وتتبع عورات الآخرين بأي وسيلة من الوسائل إلى غير ذلك من التطبيقات (عماد، 2006، ص.32).

ويمكن أن يعرف حق الخصوصية بأنه: حق الفرد أن يعيش متمتعا باحترام أشياء خاصة يطويها عن غيره في العادة، وذلك بغل يد السلطة العامة، وكذلك الأفراد عن التدخل أو التعرض لهذه الأشياء إلا في الأحوال التي تقتضيها المصلحة العامة، وذلك بإذن الشارع.

تعريف حق الخصوصية في القانون:

يرى رجال القانون أنه يصعب وضع تعريف دقيق وشامل لمفهوم حق الخصوصية؛ لأنها فكرة مرنة لا حدودلها، تعكس جوانب متعددة لحياة الإنسان، فهي تختلف من مجتمع إلى آخر، وتختلف بحسب العادات والتقاليد السائدة في الجماعة، بل وبحسب الظروف الخاصة بكل شخص من حيث كونه من الأشخاص الذين يتكتمون على خصوصياتهم أو من أولئك الذين يجعلونها كتابا مفتوحا (الخرشة، 2007، ص.378).

ومع هذا فقد عرف البعض حق الخصوصية، بأنه حق الشخص في أن يترك وشأنه أو أنه حق كل إنسان في أن يعيش حياته الخاصة بالشكل وبالإسلوب الذي يراه محققا لرغباته في حدود عدم الإضرار بالآخرين وفي الاحتفاظ بأسراره التي يرى في حجبها عن الآخرين تحقيق مصلحة له (محمد، 1988، ص.55).

ويستوي أن تنطوي الأسرار أو الخصوصيات على رذائل مستهجنة كارتكاب الجرائم الخلقية أو على أمور طبيعية تأنف الفطرة السليمة إظهارها، كالعلاقة الخاصة بين الأزواج أو حتى على أعمال كريمة مستحسنة قد يفضل أصحابها كتمانها ابتغاء مرضاة الله كالصدقات وأعمل الخير (محمد، 1988، ص.55).

المطلب الثاني: صور التعدي الإكتروني على حق الخصوصية

يمكن التعدي الإكتروني على حق الخصوصية بإحدى الطرق التالية:

- ✓ إدخال معلومات وهمية إذ يمكن بهذه الوسيلة أن يستولي المعتدي على بيانات شخصية غالبا ما تتعلق بعناصر الذمة المالية بغية تحقيق أموال لنفسه.
- ✓ التجسس الإلكتروني على الحياة الخاصة (عيسى، 2001، ص.169).
- ✓ سرقة المعلومات الخاصة وتزويرها كسرقة كلمة والمعلومات التعلقة ببطاقة الإئتمان.
- ✓ التزوير المعلوماتي عن طريق التسلل الإكتروني إلى البيانات إذ يقوم القراصنة بمحاولة الدخول إلى النظام للوصول إلى هذه المعلومات التي تكون غالبا سرية، وتجري عملية الدخول إلى النظام المعلوماتي عن طريق خرق هذه المنافذ الوصول إلى قاعدة البيانات (سوزان،2013، ص.436).
- ✓ جمع بيانات شخصية حقيقية بدون ترخيص.
- ✓ إفشاء بيانات بصورة غير قانونية وإساءة استعمالها (السنباطي، 2009، ص. 19).

هذا ومن أشهر القضايا المتعلقة بالاعتداء على حق الخصوصية، قيام الطبيب الخاص للرئيس الفرنسي السابق" فرانسوا ميتران" بتأليف كتاب عن حياة الرئيس أوضح فيه أنه كان يعلم بمرضه بالسرطان منذ بدء ولايته الأولى وبناء على طلب من أسرة الرئيس الفرنسي الأسبق حكم القضاء الفرنسي بمصادرة الكتاب نظرا لأنه يحوي ما يعد اعتداء على حرمة الحياة الخاصة للرئيس الراحل، فقام اثنان من متعهدي توفير خدمة الإنترنت ببث صورة نسخت من الكتاب الأصلي على الإنترنت فقضى القضاء الفرنسي مرة أخرى بوقف هذين المتعهدين عن العمل، وعندئذ قام آخرون ومن بينهم مركز بحثي بجامعة أمريكية في الولايات المتحدة الأمريكية بإعادة نشر ذات الكتاب على الإنترنت دفاعا عما يعد مباشرة لحرية التعبير عن الرأي، وبالتأكيد فإنه أمكن الاطلاع على الكتاب من قبل من يقيمون في فرنسا (رمضان،2000 ، ص.50).

المطلب الثالث: الوسائل التقنية لحماية حق الخصوصية

هناك عدة وسائل لحماية حق الخصوصية من أهمها ما يلي:

1. التشفير: وهو آلية يتم بمقتضاها ترجمة معلومة مفهومة إلى معلومة غير مفهومة، يمكن إرجاعها إلى حالتها الأصلية، وهو من الوسائل والأدوات المبتكرة في مجال توفير أمن وسلامة وسرية المعلومات والمعاملات والصفقات في شبكة الإنترنت.
2. ضرورية إخضاع النظم الآلية لإشراف الدولة.
3. حظر تخزين معلومات معينة على الأفراد، وإخضاع ما يجوز تخزينه لضوابط معينة.

4. تمكين صاحب الشأن من الإطلاع على المعلومات الخاصة به للتأكد من سلامتها ولتصحيح ما قد يكون بها من أخطاء (سوزان، 2013، ص.443).

المطلب الرابع: حكم الاعتداء على حق الخصوصية في الشريعة الإسلامية

حرمت الشريعة الإسلامية الاعتداء على حق الخصوصيةن فحرمت التجسس، والدخول على الغير في منزلة بغير إذنه، واستراق السمع والنظر، وقد دل على هذا الكتاب والسنة:

أولا-الكتاب:

قول الله تعالى: (يَاأَيُّهَا الَّذِينَ آمَنُوا اجْتَنِبُوا كَثِيرًا مِنَ الظَّنِّ إِنَّ بَعْضَ الظَّنِّ إِثْمٌ وَلَا تَجَسَّسُوا وَلَا يَغْتَبْ بَعْضُكُمْ بَعْضًا أَيُحِبُّ أَحَدُكُمْ أَنْ يَأْكُلَ لَحْمَ أَخِيهِ مَيْتًا فَكَرِهْتُمُوهُ وَاتَّقُوا اللَّهَ إِنَّ اللَّهَ تَوَّابٌ رَحِيمٌ) (سورة الحجرات: الآية: 12).

وجه الدلالة: دلت هذه الآية على النهي عن التجسس والبحث عن مخبآت الناس (ابن عطية،2001، ص.197).

قوله تعالى: (يَاأَيُّهَا الَّذِينَ آمَنُوا لَا تَدْخُلُوا بُيُوتًا غَيْرَ بُيُوتِكُمْ حَتَّى تَسْتَأْنِسُوا وَتُسَلِّمُوا عَلَى أَهْلِهَا ذَلِكُمْ خَيْرٌ لَكُمْ لَعَلَّكُمْ تَذَكَّرُونَ (27) فَإِنْ لَمْ تَجِدُوا فِيهَا أَحَدًا فَلَا تَدْخُلُوهَا حَتَّى يُؤْذَنَ لَكُمْ وَإِنْ قِيلَ لَكُمُ ارْجِعُوا فَارْجِعُوا هُوَ أَزْكَى لَكُمْ وَاللَّهُ بِمَا تَعْمَلُونَ عَلِيمٌ) (سورة النور: الآيات: 27،28).

وجه الدلالة: دلت هاتان الآياتان على أن الاستئذان واجب في كل حال وعلى أنه يحرم دخول البيوت المسكونة إذ لا يأمن من يهجم عليها بغير استئذان أن يرى عورات الناس، وما لا يحل النظر إليه، وهذا بلا شكش يتنافي مع الآداب الإجتماعية التي أرشد إليها الإسلام (الحنبلي، 1998، ص.451).

ثانيا السنة:

ماوري عَنْ أَبِي هُرَيْرَةَ، عَنِ النَّبِيِّ صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ قَالَ: «إِيَّاكُمْ وَالظَّنَّ، فَإِنَّ الظَّنَّ أَكْذَبُ الحَدِيثِ، وَلاَ تَحَسَّسُوا، وَلاَ تَجَسَّسُوا، ولا تنافسوا وَلاَ تَحَاسَدُوا، وَلاَ تَدَابَرُوا، وَلاَ تَبَاغَضُوا، وَكُونُوا عِبَادَ اللَّهِ إِخْوَانًا» (البخاري، 2001، ص. 2223).

وجه الدلالة:

دل هذا الحديث على حرمة التجسس والبحث عن عيوب الناس وتتبعها (العسقلاني،1988، ص.482).

ماروي عن أبي هريرة، عن النبي صلى الله عليه وسلم قال: «من اطلع في بيت قوم بغير إذنهم، فقد حل لهم أن يفقئوا عينه» (مسلم، 1995، ص.181).

وجه الدلالة:

دل هذا الحديث على أن من نظر في بيت إلى ما يقصد أهل البيت ستره، فقد حل لهم أن يرموه بشئ فيفقؤا عينه به إن لم يندفع إلا بذلك (المناوي، 1989، ص.775).

المطلب الخامس: عقوبة الاعتداء على حق الخصوصية في الشريعة الإسلامية والقانون الأفغاني

الفرع الأول: موقف الشريعة الإسلامية:

عقوبة الاعتداء على حق الخصوصية في الشريعة الإسلامية عقوبةتعزيرية يوكل تقديرها إلى الإمام، فيختار ما يناسب حجم الضرر الواقع على الغير، فله الحبس، والنفي، والإعراض عن الجاني وتوبيخه والتشهير به وله أيضا المعاقبة بالغرامة المالية (بركة، 2008، ص.63).

الفرع الثاني: موقف القانون الأفغاني:

لم ينص المشرع على عقوبة جديدة لجريمة الاعتداء على حق الخصوصية المرتكبة عبر شبكة الإنترنت، ولذلك يتم اللجوء في هذا الشأن إلى المواد المنظمة للعقوبة المقررة لجريمة الاعتداء على حق الخصوصية التقليدية (أنور، 2010، ص.7).

وقد نصت المادة (181) من قانون العقوبات الأفغاني، على مايلي:

"يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدي على حرمة حق الخصوصية للمواطن، ولذلك بأن ارتكب أحد الأفعال الآتية، في غير الأحوال المصرح بها قانونا أو بغير رضاء المجني عليه:

1) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

2) التقط أو نقل بجهاز من الأجهزة أيا كان نوعه صورة شخص في مكان خاص.

فإذا صدرت الأفعال المشار إلها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأي من الحاضرين في ذلك الإجتماع فإن رضاء هؤلاء يكون مفترضا. ويعاقب بالحبس الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادا على سلطة وظيفته، ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها (مصطفى، 2011، ص. 435).

الفرع الثالث: الموازنة بين الشريعة والقانون

تتفق كل من الشريعة الإسلامية والقانون الوضعي الأفغاني على أن عقوبة الاعتداء على حق الخصوصية في كل منهما تعزيرية وتختلف الشريعة عن القانون في أن العقوبة يقدرها القاضي؛ لأن المقصود من التعزير الزجر وأحوال الناس فيه مختلفة، والقانون الوضعي حدد عقوبة للاعتداء على حق الخصوصية متمثلة في الحبس كما سبق.

نتائج البحث:

أن الإنترنت: شبكة عالمية عملاقة تربط الملايين من أجهزة الحاسب الآلي المنتشرة حول العالم ببعضها من أجل تبادل المعلومات.

- ✓ من خصائص شبكة الإنترنت أنها ليست مملوكة لأحد، وعدد المستخدمين لها في تزايد مستمر، وأنها عابرة للحدود.
- ✓ جريمة الإنترنت: هي كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو نقلها.

✓ من جرائم الإنترنت الاعتداء على حق الخصوصية ويمكن الاعتداء بعدة طرق منها، إدخال معلومات وهمية، والتجسس الإلكتروني، وسرقة المعلومات الخاصة وتزويرها وجمع بيانات شخصية حقيقية بدون ترخيص، وإفشاء بيانات بصورة غير قانونية.

✓ يمكن حماية حق الخصوصية بعدة وسائل منها، التشفير، وإخضاع النظم الآلية لإشراف الدولة، وحظر تخزين معلومات معينة على الأفراد.

✓ حرمت الشريعة الإسلامية الاعتداء حق الخصوصية، فحرمت التجسس، والدخول على الغير في منزله بغير إذنه، واستراق السمع والنظر.

✓ عقوبة الاعتداء على حق الخصوصية في الشريعة الإسلامية عقوبة تعزيرية يوكل تقديرها إلى الإمام.

✓ يعاقب القانون الأفغاني على الاعتداء على حق الخصوصية بالحبس مدة لا تزيد على سنة.

قائمة المراجع:

1) القرآن الكريم

2) ابن منظور، محمد بن مكرم الأفريقي المصري. (1994). لسان العرب، دار صادر- بيروت الطبعة الأولى.

3) أنور، فتحي محمد. (2010). تفتيش الأمنية لجرائم الإنترنت لضبط جرائم الاعتداء على الآداب العامة والشرف والاعتبار التي تقع بواسطتها.

4) البخاري، محمد بن إسماعيل أبو عبد الله الجعفي. (ه1422). المحقق: محمد زهير بن ناصر الناصر، صحيح البخاري، دار طوق النجاة (مصورة عن السلطانية بإضافة ترقيم تمحمد فؤاد عبد الباقي

5) بركة، إيمان، ومحمد سلامة. (2008). الجريمة الإعلامية في الفقه الإسلامي. رسالة ماجستير، الجامعة الإسلامية بغزة، فلسطين

6) التميمي، محمد خليفة. تطوير التعليم الإسلامي عن طريق الإنترنت وتجربة جامعة المدينة العالمية في التعليم عن بعد بماليزيا. بحث منشور على موقع www.cis.psu.ac.th.

7) الحنبلي، أبو حفص، وسراج الدين، عمر بن علي بن عادل الحنبلي الدمشقي النعماني. (1998). المحقق: الشيخ عادل أحمد عبد الموجود والشيخ علي محمد معوض.اللباب في علوم الكتاب. بيروت: دار الكتب العلمية

8) الخرشة، محمد أمين فلاح. (2007). جرائم الاعتداء على الحق في الحياة الخاصة في قانون العقوبات الأردني. مجلة الحقوق. جامعة مؤته

9) السبق، عبد الكريم قاسم. (2003). مدى استقادة الأجهزة الأمنية من خدمات شبكة الإنترنت. رسالة ماجستير، أكاديمية نايف العربية للعلوم الأمنية

10) سلطان، محمد سيد. (2012). قضايا قانونية في أمن المعلومات وحماية البيئة الالكترونية.د.م.: دار ناشري للنشر الإلكتروني

11) السنباطي، عطاء. (2009). موقف الشريعة الإسلامية من جرائم الحاسب الآلي والإنترنت.دم.: دار النهضة العربية

12) سوزان، عدنان. (2013). انتهاك حرمة الحياة الخاصة عبر الإنترنت. مجلة جامعة دمشق للعلوم الإقتصادية والقانونية، 29(3).

13) الصابوني، محمد علي. (1980). روائع البيان تفسير آيات الأحكام(ط.3). دمشق: مكتبة الغزالي

14) صغير، يوسف. (2013). الجريمة المرتكبة عبر الإنترنت. رسالة ماجستير السياسية جامعة مولود معمري – تيزي وزو، الجزائر

15) العبودي، محس. (2014). المواجهة الأمنية لجرائم الإنترنت. منشور على موقع: www.eastlaws.com

16) العجمي، عبد الله دغش. (2014). المشكلات العملية والقانونية للجرائم الإكترونية" دراسة مقارنة". رسالة ماجستير، جامعة الشرق الأوسط

17) العسقلاني، الإمام الحافظ أحمد بن على بن حجر. (1379ه). فتح الباري شرح صحيح البخاري. بيروت: دار المعرفة

18) عماد، أحمد حمدي محمود. (2006). الحق في الحصوصية ومسئولية الصحفي في ضوء احكام الشريعة الإسلامية والقانون المدني دراسة مقارنة. أطروحة دكتوراة، كلية الشريعة والقانون، القاهرة

19) عيسى، طوني. (2001). التظيم القانون لشبكة الإنترنت، دراسة مقارنة في ضوء القوانين الوضعية والاتفاقيات الدولية.دم: منشورات الحلبي الحقوقية

20) الغافري، حسين بن سيف. (2009). السياسية الجنائية في مواجهة جرائم الإنترنت" دراسة مقارنة". أطروحة دكتوراة، كلية الحقوق، جامعة عين شمس، القاهرة

21) غلاييبي، عارف.الجريمة المنظمة وأساليب مكافحتها، بحث مقدم لمعهد قوي الأمن الداخلي 2008م، منشور على موقع : mohammed@minshawi.com.

22) الفارابي، أبو نصر إسماعيل بن حماد الجوهري. (1987). الصحاح تاج اللغة وصحاح العربية(ط.4). بيروت: دار العلم للملايين

23) قانون العقوبات الأفغاني 2018م.

24) الماوردي، علي بن محمد بن محمد بن حبيب البصري البعدادي. الأحكام السلطانية. القاهرة: دار الحديث

25) المحاربي، أبو محمد عبد الحق بن غالب بن عبد الرحمن بن تمام بن عطية الأندلسي. (1422). المحرر الوجيز في تفسير الكتاب العزيز. بيروت: دار الكتب العلمية

26) محمد، عبد العظيم. (1988). حرمة الحياة الخاصة في ظل التطور العلمي الحديث دراسة مقارنة. أطروحة دكتوراه، جامعة القاهرة، القاهرة

27) مسلم، أبو الحسن القشيري بن الحجاج النيسابوري، ومحمد، فؤاد عبد الباقي. (1995). صحيح مسلم. بيروت: دار إحياء التراث العربي

28) هميم، عبد اللطيف. (1981). جرائم الاعتداء على الحياة الخاصة وعقوبتها في الشريعة والقانون. رسالة ماجستير كلية الشريعة والقانون، القاهرة

الإطار القانوني والإجرائي للجنوح السيبراني للأطفال في ظل القانون رقم 15-12 في الجزائر

The legal and procedural framework for cyber-delinquency of children under Law 12.15 in Algeria

د.عائشة عبد الحميد/ جامعة الشادلي بن جديد، الطارف/ الجزائر
Dr.Aicha AbdelHamid/Chadli Ben Djedid University, Taref / Algeria

ملخص الدراسة:

يوجه المشرع الجزائري في الآونة الأخيرة انتباها خاصا لفئة الأطفال نتيجة للتطور الخطير لأشكال الاعتداء عليهم بالإضافة إلى بعض التعديلات الجوهرية التي أضافها إلى قانون العقوبات، أصدر في سنة 2015 قانونا خاصا بحماية الطفل، يتضمن أحكاما حماية خاصة سواء من الناحية الاجتماعية أو القانونية، لكن المشرع نص على التجريم فيما يتعلق بالجرائم الماسة بكرامة الطفل كحماية من الإهمال المادي أو المعنوي، ترك الأطفال، الاعتداء على الأطفال وغيرها.

ولكن ماذا عن ارتكاب الطفل للجريمة أو ما يوصف بجنوح الأحداث، خاصة فيما يتعلق بالجرائم الإلكترونية المرتبطة أساسا بالتكنولوجيا والتي تصل إلى درجة انتحار الأطفال أو مختلف الجرائم الأخرى المرتبطة بالأشخاص والأموال كالقتل والسرقة.

الكلمات المفتاحية: الجنوح السيبراني، الأطفال، التشريع الجزائري، التكنولوجيا، قانون العقوبات.

Abstract:

The Algerian lawmaker has recently paid special attention to children because of the dangerous development of forms of abuse against them in addition to some fundamental amendments that he added to the penal code. On the criminalization of crimes against the dignity of the child as protection from material or moral neglect, abandonment of children, child abuse, ect.

But what about the child's commission of the crime or what is described as juvenile delinquency, especially with regard to cyber crimes related mainly to technology and which reach the point of child suicide or various other crimes related to people and money such as murder and theft.

Keywords: Cyber delinquency, children , Algerian legislation, technology, the penal code.

مقدمة:

يعتبر الحاسوب أو الهاتف والإنترنيت من إنجازات تكنولوجيا المعلومات، التي أعادت تشكيل حياة الطفل في البيت والمدرسة، فقد أصبح أطفال المجتمع الإلكتروني عرضة لإيجابيات وسلبيات ذلك المجتمع. (غياث، ومرباح، 2019، ص. 267)

ما يميز الطفل في هذه المرحلة هو حصوله على بعض المعلومات وتقدمه في السن، وتبعا لذلك اكتسابه شخصيته أكثر رسوخا. (دردوس، 1979، ص. 196)

فتحديد سن الحدث هو الفيصل في تحديد مسؤوليته الجزائية سواء من حيث المسؤولية الكاملة أو مسؤوليته كصغير وهل نطبق بحقه التدابير والعقوبات وحسب النظام القانوني الخاص به. فالعبرة في تحديد سن الحدث هي بلحظة وقوع الجريمة. (صقر، وحبلي، 2008، ص. 19)

تعاني كثير من الأسر في الدول النامية من التفكك حيث تعيش في حرمان وبؤس وجهل نتيجة الفقر أو الحروب الأهلية أو الهجرة، وينتشر الأطفال في الشوارع للتسول، مما يسهل عليهم الخطف والتهريب وتجارة المخدرات وغيرها من الجرائم. (العشاوي، 2011، ص. 317)

حيث تعد تصرفات الطفل العدوانية منت المواضيع المهمة وموضوع مهم البحث الجنائي والاجتماعي حيث يتأثر الطفل في سلوكه العدواني بالظروف الاجتماعية والعائلية. (Al-Ma'seb, Alsejari, Al-Quand, 2013, P.9)

ورد مصطلح " الطفل " ومصطلح الطفولة في العديد من الإعلانات والاتفاقيات الدولية لحقوق الإنسان والاتفاقيات المتعلقة بالقانون الدولي الإنساني، وبإعلان جنيف لحقوق الطفل لعام 1924، ثم إعلان حقوق الطفل لعام 1959، والعهد الدولي الخاص بالحقوق الاقتصادية والثقافية والاجتماعية والعهد الدولي للحقوق المدنية والسياسية لعام 1966، إلا أنها لم تحدد المقصود بهاذين المصطلحين ولا الحد الأقصى لسن الطفل أو نهاية مرحلة الطفولة، إلى أن جاءت إتفاقية حقوق الطفل التي تبنتها الجمعية العامة للأمم المتحدة بالإجماع في 20 نوفمبر 1989، فقد عرفت المادة الأولى الطفل بأنه:" كل إنسان لم يتجاوز الثامنة عشر، ما لم يبلغ سن الرشد قبل ذلك بموجب القانون المطبق عليه".(عبد الحميد، 2018، ص. 97)

وعلى ذلك نطرح الإشكالية التالية: -كيف عالج المشرع الجزائري حالة الجنوح السيبراني لدى الأطفال ؟.

انتهجنا لذلك منهجا تحليليا ووصفيا للدراسة.

أولا-الإجراءات الخاصة بالجنوح السيبراني للأطفال:

إن التطور المذهل جعل التشريعات الجنائية العالمية عاجزة على موجهة مثل هذا النوع من الجرائم ونتيجة لخصوصيتها وطابعها غير الملموس يتعذر تطبيق النصوص التقليدية لقانون العقوبات، وأية محاولة لتحميلها بما لا يطابق، قد تصطدم بمبدأ الشرعية، لذا بدأ المشرعون ينتبهون إلى ضرورة محاصرة الإجرام المعلوماتي بقواعد جديدة ونصوص تتلاءم مع طبيعتها الخاصة.

ولعل التشريع الجزائري يعتبر من الأوائل الذين تفطنوا إلى هذا النوع من الإجرام والفراغ التشريعي الذي أحدثه، حيث سارع بدوره إلى تعديل قانون العقوبات سنة 2004 وأورد قسما جديدا تحت عنوان المساس بأنظمة المعالجة الآلية للمعطيات في المواد من 394 مكرر إلى 394 مكرر 7 من قانون العقوبات الجزائري. (الأمر رقم 66-156 المؤرخ في 08 يونيو 1966)

1.توقيف الأطفال كإجراء احترازي عند ارتكاب الجرائم:

بالإضافة لتنظيم قانون الإجراءات الجزائية الجزائر (الأمر رقم 66-155 المؤرخ في 08 يونيو 1966) التوقيف للنظر في المواد 1/51، 2، 3 والمادة 141 في التلبس، والبحث الأولي، والإنابة القضائية، فإن التوقيف للنظر نظمه أيضا

القانون المتعلق بحماية الطفل، رقم 15-12 المؤرخ في 15 يوليو 2015، فالمادة الأولى منه تعرف الطفل بأنه " كل شخص لم يبلغ الثامنة (18) عشر سنة كاملة ".

أما الطفل الجانح فهو الطفل الذي يرتكب فعلا مجرما والذي لا يقل عمره عن 10 سنوات ".

والعبرة بتحديد سن الطفل الجانح هو يوم ارتكاب الجريمة، حيث لا يخضع الطفل الجانح لنفس الإجراءات المطبقة على حالة التلبس في الجرائم، بل تموضع أحكام خاصة بالطفل.

أ) -الأحكام الخاصة:

يخضع التوقيف للنظر للطفل الجانح على النحو التالي:

- ✓ عدم تطبيق إجراءات التلبس بالجريمة على الجرائم التي يرتكبها الطفل حتى ولو كانت جناية طبقا للمادة 2/64 من قانون حماية الطفل.
- ✓ التوقيف للنظر لا يطبق على حالة الاشتباه بالطفل الجانح، إذا لم يبلغ 13 سنة كاملة.
- ✓ إذا استدعت مقتضيات التحري الأولي، يجوز لضباط الشرطة القضائية أن يوقف الطفل للنظر الذي يبلغ 13 سنة كاملة على الأقل طبقا للمادة 48 من قانون حماية الطفل.
- ✓ يتم توقيف الحدث الجانح الذي بلغ 13 سنة في أماكن مستقلة عن أماكن توقيف البالغين.
- ✓ مدة التوقيف للنظر إلا في الجنح التي تشكل إخلالا ظاهر بالنظام العام.
- ✓ إخطار ممثله الشرعي بكل الوسائل.
- ✓ إجبارية إجراء الفحص الطبي للطفل الموقوف.
- ✓ حق المشتبه فيه الحدث الموقوف تحت النظر في الاستعانة بمحام، وهو حضور وجوبي بغرض مساعدته، غير أنه استثناءا يجوز سماع أقوال الطفل الجانح بدون وجود محام في حالتين هما:
  - الحصول على إذن من وكيل الجمهورية لسماعه بعد مضي ساعتين من التوقيف.
  - إذا كان الحدث عمره بين 16 و18 سنة، وكان ينسب إليه أعمال ذات صلة بالإرهاب والتخريب أو المتاجرة بالمخدرات أو أفعال ارتكبت في جماعة إجرامية منظمة.
- ✓ يعتبر الإخلال بإجراء الفحص الطبي أو انتهاك آجال التوقيف للنظر كما هو منصوص عليه في المادة 49 من قانون حماية الطفل جريمة، تعرض ضباط الشرطة القضائية لعقوبة الحبس. (غاي، 2005، ص. 27)

ب) -الأحكام العامة:

بالإضافة للأحكام الخاصة للتوقيف للنظر للحدث الذي يبلغ 13 سنة ولم يبلغ سن الرشد الجزائي، يقرر قانون حماية الطفل في أحوال معينة تطبيق الأحكام العامة في قانون الإجراءات الجزائية على النحو التالي:

- ➢ يخضع الحدث في توقيفه لإجراء البحث والتحري أو التحقيق الأولي المنصوص عليها في المادة 65 من قانون الإجراءات الجزائية.

كما تخضع إجراءات تمديد التوقيف للنظر للشروط والكيفيات المنصوص عليها في قانون الإجراءات الجزائية.

- ➢ يجب على ضباط الشرطة القضائية بمجرد توقيف طفل للنظر، إخطار ممثله الشرعي بكافة الوسائل.

- إعلام الطفل بحقه في طلب فحص طبي أثناء التوقيف للنظر.
- يمكن لوكيل الجمهورية سواء من تلقاء نفسه أو بناءا على طلب من الطفل أو ممثله الشرعي أو محاميه أن يندب طبيبا لفحص الطفل في أية لحظة أثناء التحقيق للنظر. (أوهايبية، 2018، ص. 380)
- يقرر قانون الإجراءات الجزائية الجزائري لضباط الشرطة القضائية مهما كانت جهة انتمائهم الأصلية، سواء كانوا من جهاز الدرك الوطني أو من جهاز الأمن الوطني أو من مصالح الأمن العسكري اختصاصا وطنيا، في البحث والتحري ومعاينة بعض الجرائم الموصوفة، ومن ضمن هذه الجرائم الموصوفة، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات (الجرائم الإلكترونية) طبقا لنص المادة 15 من قانون الإجراءات الجزائية ، حيث يكون لهؤلاء اختصاص وطني خاص، يخولهم البحث والتحري عن جرائم ومجرمين ومعاينتها على مستوى الإقليم الوطني.(هنوني، يقدح، 2011، ص. 27)

2. الجرائم التي يقوم بها الحدث طبقا للتشريع الجزائري:

إن مراحل التطور المختلفة للإنسان وما يصاحبها من تغيرات في التكوين العضوي، وما يتبعه من تغير أيضا في البيئة، له تأثير على ظاهرة الإجرام، فأطوار السن المختلفة تصاحبها تغيرات عضوية تؤثر في التكوين النفسي، وبالتالي في الأطوار الإجرامية للشخص (سلامة، 1979، ص203) ومنها:

أ) -جرائم ضد الأشخاص:

يعد الاعتداء على الأشخاص بمثابة الجرائم التي تهدد الحقوق الشخصية للمجني عليه، ويرجع ارتكاب الحدث لمثل هذه الجرائم، إلى معاملة بقسوة داخل الأسرة والشارع، بالإضافة إلى المؤثرات الثقافية التي تدفع به إلى العنف الذي يزداد في فترة المراهقة بين 14-17 سنة، أين تزداد القوة البدنية للحدث فستعملها للاعتداء على غيره دون إدراك عواقب فعله، لعدم توافر القدرة الفكرية التي تمنعه من ذلك، وقد أثبتت دراسة لجنوح الأحداث في الجزائر أجريت سنة 1979 بأن 93% من الأحداث الجانحين تتراوح أعمارهم ما بين 16 و17 سنة.

ب) -الجرائم المرتكبة ضد الأموال:

إن هذا النوع من الجرائم، يعد من أيسر الجرائم التي يرتكبها الحدث، لأنها لا تتطلب أكثر من المغامرة والجرأة لتغطية موارده المالية المحدودة، ويدخل في نطاق الاعتداء ضد الأموال زيادة على تهديد الحقوق ذات القيمة المالية، خيانة الأمانة، تخريب ملك الغير، الإخفاء والحريق، ولكل أكثر جريمة مرتكبة من قبل الأحداث هي جريمة السرقة.

فالحدث في فترة المراهقة يتميز بالتزامات نفسية تلازمه، فيجذبه عاملان متناقضان، أحدهما يدفعه للانسجام والتوافق الاجتماعي، بينما يميل الآخر به للتحرر من كل قيد ونظام، وتحيط به حالات نفسية خطيرة أهمها الغيرة والحسد، المغامرة والشك وسرعة الغضب.

ج) -جرائم ضد الأخلاق:

حيث يقوم الحدث بهذه الجرائم نتيجة الكبت والصراع بين الرغبات الجنسية، والخلق الساقط عند بعض الأسر والمحيط الخارجي، فعند نضج الغريزة الجنسية لدى الحدث يدفعه فضوله وجهله للأمور الجنسية إلى اكتشاف

هذا التغيير الذي لا يتفق في كل الأحوال مع القانون، كما أن الحدث يعمد إلى التمرد على القيود المفروضة عليه، فتضعف عنده القدرة على ضبط النفس. (أوذاينية، وغربي، 2013، ص. 56)

ثانيا-خضوع الطفل لأحكام قانون العقوبات رقم 05-11 المؤرخ في 17 يوليو 2005 فيما يتعلق بجرائم التكنولوجيا:

عملا بقانون التنظيم القضائي الجديد المعدل وقانون حماية الطفل، فإن القضاء المتخصص يتكون من محكمة الجنايات الابتدائية ومحكمة الجنايات الاستئنافية، وقضاء الأطفال أو الأحداث والجهات القضائية العسكرية. (أوهايبية، 2018، ص. 196)

وبالرجوع إلى قانون حماية الطفل (القانون رقم 15-12 المؤرخ في 15 يوليو 2015 يتعلق بحماية الطفل، ج.ر عدد 41 لسنة 2015)، فإن الطفل الجانح يخضع لإجراءات خاصة طبقا للمادة 62 من قانون حماية الطفل بقولها:" يمارس وكيل الجمهورية الدعوى العمومية لمتابعة الجرائم التي يرتكبها الأطفال، وأضافت المادة 64 من نفس القانون " يكون التحقيق إجباريا في الجنح والجنايات المرتكبة من قبل الطفل ويكون جوازيا في المخالفات".

كما تم استبعاد تطبيق أحكام المثول الفوري على الطفل الجانح بحكم المادة 64 من قانون حماية الطفل، والمادة 339 مكرر بوجوب التحقيق في جنح الأطفال فتنص الأولى: " يكون التحقيق إجباريا في الجنح والجنايات المرتكبة من قبل الطفل ".

1. أنواع الجرائم المرتبطة بالتكنولوجيا والمعلومات:

نجد الآتي:

- جريمة التوصل بطريقة الغش لنظام المعالجة الآلية للمعطيات:

نصت عليها المادة 394 مكرر من قانون العقوبات، حيث يعاقب بالحبس من 03 أشهر إلى سنة وبغرامة من 50.000 دج إلى 100.000 دج كل من يدخل أو يبقي عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو يحاول ذلك.

- جريمة الإتلاف العمدي المعلومات:

تعاقب وتنص عليها المادة 394 مكرر 1 من قانون العقوبات، حيث يعاقب كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية وأزال أو عدل بطريق الغش المعطيات التي يتضمنها.

فالمشرع الجزائري قد حقق قفزة نوعية في مجال التجريم المعلوماتي، لأن الخطورة الإجرامية التي تنبأ بها هذه الظاهرة تتعدى في جسامتها أشكال الإجرام التقليدي وأنها تستهدف أساسا مجالات حساسة في الدولة. (طباش، 2014، ص.293)

2.الجانب العقابي لجرائم التكنولوجيا لدى الأطفال:

إذا ما تصفحنا القانون العقابي الجزائري، أو قانون حماية الطفل لا نجد النص على العقوبات المطبقة على الطفل الجانح في مجال الجرائم المرتبطة بالتكنولوجيا، لذلك وجب الرجوع إلى القواعد العامة فيما يتعلق بالعقوبات والإجراءات المطبقة على الأطفال:

أ) -العقوبات المطبقة على الجرائم التكنولوجية بشكل عام:

عادة ما يقسم الجزاء الجنائي إلى نوعين/ عقوبة أصلية وعقوبة تكميلية.

- **العقوبة الأصلية:** العقوبة الأصلية هي الإعدام والمؤبد، والسجن المؤقت أو المؤبد.

ويعد الحبس عقوبة سالبة للحرية ومانعة لها سواء كان مؤبدا أو مؤقتا. حيث يعاقب المشرع الجزائري على الجريمة التكنولوجية أو المرتبطة بأنظمة المعلومات بالحبس الذي يتراوح مدته من 03 أشهر إلى 03 سنوات، بالإضافة إلى العقوبة المالية وهي الغرامة.

- **العقوبة التكميلية:** لقد أضاف القانون رقم 09-04 المؤرخ في 05 أوت 2009، والمتضمن القواعد الخاصة بالوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتهما، التدخل الفوري لسحب وتخزين المحتويات. (أوهايبية، 2015، ص. 405)

ب) -العقوبات المطبقة على الطفل الجانح بالرجوع إلى القواعد العامة لقانون العقوبات:

لم ينص كل من قانون العقوبات، والقانون رقم 09-04، وقانون حماية الطفل على العقوبات المطبقة على الطفل في حال ارتكابه جرائم متعلقة بالتكنولوجيا، لذا وجب الرجوع للقواعد العامة.

- **صغر السن مانع من موانع المسؤولية:**

يعتبر صغر السن في التشريعات العقابية الحديثة مانعا من موانع المسؤولية الجنائية طبقا لنص المادة 442 من ق.إ.ج.

أما إذا كان القاصر يبلغ من العمل من 13 إلى 18 سنة فإنه يخضع طبقا للمادة 49 من قانون العقوبات، إما لتدابير الحماية أو التهذيب أو لعقوبات مخففة.

- **تسليط نص العقوبة على الحدث الجانح:**

طبقا للمادتين 50، 51 من العقوبات، فإن الحدث الجانح الذي يبلغ من العمر من 13 إلى 18 سنة، عند تعرضه لحكم جزائي، فإن العقوبة التي تصدر ضده تكون كالآتي:

- إذا كانت العقوبة التي تفرض عليه هي الإعدام أو السجن المؤبد فإنه يحكم عليه بعقوبة الحبس من 10 سنوات إلى 20 سنة.
- إذا كانت العقوبة هي السجن أو الحبس المؤقت فإنه يحكم عليه لمدة تساوي نصف المدة التي يتعين الحكم بها على شخص بالغ

خاتمة:

هدفنا من خلال الدراسة إلى إلقاء الضوء على حالة جنوح الأطفال في الجرائم السيبرانية المرتبطة بالتكنولوجيا، حيث وجه المشرع الجزائري اهتماما خاصا بجرائم المعلومات، ولكنه من جهة أخرى أهمل الجرائم المعلوماتية الخاصة بالأطفال بذلك نخلص إلى النتائج التالية:

- ✓ عمد المشرع الجزائري إلى تعديل قانون العقوبات لتسليط الضوء على الجرائم المعلوماتية.
- ✓ عدل المشرع الجزائري قانون الطفل حيث هدف إلى حماية الطفل ولكنه أهمل الجانب الإجرامي للطفل.

✓ بالرجوع إلى قانون العقوبات والقانون الخاص بالوقاية من الجرائم المعلوماتية نجده خاليا من مصطلح الطفل.

✓ ونوصي بما يلي:

✓ إن تحديد مصطلح الطفل لا يقل أهمية عن تحديد مصطلح الطفل الجانح في التشريع العقابي الجزائري.

✓ ضرورة مواكبة التكنولوجيا الحالية وإدخال مصطلح الطفل الجانح للقانون 09-04.

قائمة المراجع:

1) غاي، أحمد. (2005). التوقيف للنظر، سلسلة ضباط الشرطة القضائية. الجزائر: دار هومة

2) دردوس، مكي. (1979). الموجز في علم الإجرام. الجزائر: ديوان المطبوعات الجامعي

3) العشاوي، عبد العزيز. (2011). حقوق الإنسان في القانون الدولي. الجزائر: دار الخلدونية

4) أوهايبية، عبد الله. (2018). شرح قانون الإجراءات الجزائية الجزائري. الجزائر: دار هومة

5) أوهايبية، عبد الله. (2018). شرح قانون الإجراءات الجزائية الجزائري. الجزائر: دار هومة

6) أوهايبية، عبد الله. (2015). شرح قانون العقوبات الجزائري: القسم العام. الجزائر: ENAG للنشر

7) طباس، عز الدين. (2014). شرح الجزء الخاص من قانون العقوبات. الجزائر: د.ن.

8) مأمون، محمد سلامة. (1979). أصول علم الإجرام وعلم العقاب. القاهرة: دار الفكر العربي

9) صقر، نبيل، وحبلي، صابر. (2008). الأحداث في التشريع الجزائري، الجزائر: دار الهدى

10) هوني، نصر الدين، ويقدح، دارين. (2011). الضبطية القضائية في القانون الجزائري(ط.2). الجزائر: دار هومة الجزائر

11) أوذاينية، سناء، وغربي، مجدي. (2013). المسؤولية الجزائية للأحداث في ظل التشريع الجزائري، مذكرة ماستر، جامعة محمد الشريف مساعدية، سوق أهراس، الجزائر

12) عبد الحميد، عائشة. (2018). انتهاك قوات التحالف للقانون الدولي الإنساني في العراق. أطروحة دكتوراه، جامعة باجي مختار، عنابة، الجزائر

13) غياث، حياة، ومرباح، فاطمة الزهراء. (2019). الجرائم الإلكترونية الحديثة وإشكالية التعامل معها، تحدي الحوت الأزرق وظاهرة إنتحار الأطفال في الجزائر. مجلة دراسات إنسانية واجتماعية، جامعة وهران

14) الأمر رقم 66-155 المؤرخ في 08 يونيو 1966، المتضمن قانون الإجراءات الجزائية المعدل والمتمم.

15) الأمر رقم 66-156 المؤرخ في 08 يونيو 1966، المتضمن قانون العقوبات الجزائري المعدل والمتمم.

16) القانون رقم 15-12 المؤرخ في 15 يوليو 2015 يتعلق بحماية الطفل، الجريدة الرسمية عدد 41 لسنة 2015.

17) Hen Al-Ma'seb, maha، &Alsejari, Ibtisam Al-Quand. (2013) .The effect of Ge، der on Aggressive behaviors among khuwaiti cjildren, journal of social sciences.

المسؤولية الناشئة عن التنمر الإلكتروني

Liability resulting from cyberbullying

م.م.أوج عماد صبري/كلية القانون، جامعة البيان/العراق
Asst.Lect.Awj Emad Sabri Alubaydi/ College of Law, Al-Bayan University/ Iraq

د.صابرين يوسف عبد الله/ كلية القانون، جامعة البيان/العراق
Dr.Sabreen Yousif Abdullah Al-Hayani/College of Law, Al-Bayan University/ Iraq

ملخص الدراسة:

أن التنمر الإلكتروني ظاهرة مستحدثة انتشرت على نطاق واسع عبر شبكة الانترنت، وأصبحت تشكل تهديدا لحقوق الأفراد وحرياتهم، دون أن تكون هنالك نصوص قانونية تعاقب عليها، وغالبا ما ينشأ عنها أضرار معنوية بالغة الجسامة، الأمر الذي يقتضي من المشرع أن يتدخل لسن قوانين تكفل الحد منها، وسنعتمد على المنهجين التحليل والمقارن لدراسة هذه الظاهرة في القانونين المصري والفرنسي، للتعرف على الحلول التي استخدمتها في مواجهة التنمر؛ لأجل الاستفادة منها ووضع حد لخطورتها المتزايدة في العراق، وقد حددت الدول أشكال متعددة للسلوك الإجرامي الذي يمكن أن ترتكب هذه الظاهرة من خلاله، ورتبت على ارتكابه مسؤولية جزائية تمثلت بالعقوبات ومسؤولية مدنية تمثلت بالتعويض.

الكلمات المفتاحية: تنمر، متنمرون، ضحية، جريمة، إلكترونية، مسؤولية

Abstract :

Cyberbullying is a new phenomenon that has spread widely across the Internet, and it become a threat to the rights and freedoms of individuals, without a legal rules that punish on it, and it often caused a very serious moral damage, and that imposed on the legislator to intervene to enact laws to ensure face it. We will base on the analytical and comparative method to study this phenomenon in the Egyptian and French laws, to identify the solutions that they used in the face of bullying; In order to take advantage of it and put an end to its increasing danger in Iraq, countries have identified multiple forms of criminal behavior through which this phenomenon can be committed, and have decided criminal responsibility represented by penalties and civil responsibility represented by indemnity

keywords: Bullying , Bullies , Victim , Crime , Cyber , Liability

مقدمة:

يعد التنمر الإلكتروني من المصطلحات الحديثة التي دخلت في نطاق القوانين العقابية كأثر لتطور تقنية المعلومات الحديثة، إذ الملاحظ أنه كلما كان هنالك تقدما في مستوى التكنولوجيا الحديثة كلما رافق ذلك ظهور أنماطا مستحدثة من الأفعال الإجرامية التي تستهدف النيل من حقوق الأفراد وحرياتهم، ويرجع ذلك إلى السهولة الكبيرة في استخدام تلك التقنيات فضلا عن القدرة العالية على التخفي، والتي تمكن الجاني من أن يرتكب جريمته دون أن تكون شخصيته معروفة بالنسبة للضحية أو الجهات القانونية، وغالبا ما يكون ذلك دافعا للجناة نحو التمادي في ارتكاب

هذه الجرائم، وقد يرتكب الجاني العشرات من الجرائم دون أن يلاقي جزاءً على أياً منها، وكلما تطورت وسائل تقنية المعلومات الحديثة وازدادت خبرة الجاني في هذا المجال كلما زادت جرائمه من حيث الكم والنوع وتطورت من حيث طريقة الارتكاب وبما يضمن لنفسه عدم الكشف عن هويته.

مشكلة البحث وأسئلته:

تتمثل مشكلة البحث بانتشار ظاهر التنمر الإلكتروني على نطاق واسع، وتهديدها لحقوق وحريات الأفراد دون أن تكون هنالك نصوص قانونية رادعة للجناة، وأن وجدت في بعض التشريعات فأنها ليست بالدرجة التي تحقق الحد منها، مما يكشف عن وجود فراغ أو ثغرة تشريعية في معالجة هذه الظاهرة التي تزايدت مخاطرها بشكل ملحوظ وخاصة في الآونة الأخيرة، الأمر الذي يستدعي من المشرع أن يتدخل بتنظيمها وفق نصوص عقابية حازمة تكفل معالجة حقيقية لانتشارها غير المحدود عبر مواقع التواصل الاجتماعي، ولاسيما أنها في الغالب ترتكب من قبل مراهقين لا يقدرون مسؤولية أفعالهم، وتوجه ضد ضحايا من أعمارهم أو أقل، وتسبب أضرار معنوية بالغة لهم، قد تدفع بالضحية إلى الانتحار أو تعرضه لضغوطات نفسية وخاصة إذا كانوا طلبة في المراحل الدراسية المختلفة، وهو ما يكشف عن الأبعاد الحقيقية لخطورة هذه الظاهرة، ويمكننا أن نجمل تساؤلات الدراسة بالآتي: ما المقصود بالتنمر الإلكتروني؟ ومن هو أول من صاغ هذا المصطلح؟ وبماذا يختلف عن التنمر التقليدي؟ وهل يعد التنمر الإلكتروني جريمة في القانون العراقي والقوانين المقارنة؟ وما هي الآثار التي يمكن أن تنشأ عن ارتكابه؟

أهمية البحث وأهدافه:

تظهر أهمية هذا البحث في كونه يسعى إلى تسليط الضوء على هذه الظاهرة الخطيرة من أجل لفت الأنظار نحو التصدي لها والعمل على وضع الحلول العلاجية والوقائية للقضاء عليها أو التخفيف من حدتها، سواء أكان ذلك بتشريع قانوني جديد خاص يعاقب عليها، أم بتعديل قانون العقوبات النافذ وشمولها ضمن نصوصه بمادة تضاف إليه، أما هدف البحث فهو توفير حماية قانونية كافية لحقوق الأفراد وحرياتهم ضد الانتهاكات الخطيرة التي باتت تمس الإنسان في أغلى ما يملك: في كرامته، اعتباره الاجتماعي، شرفه وسمعته، وبعبارة أخرى تمس كيانه المعنوي بأكمله، وتسبب له أضرار بالغة ليس من السهل أن تزال آثارها، كونها تمارس عبر شبكة الاتصالات الحديثة وتكون متاحة لجميع من لهم صلة به، وتبعا لذلك تكون أضرارها أبلغ مما لو ارتكبت وجها لوجه.

منهجية البحث:

سنعتمد في بحث موضوع التنمر الإلكتروني على المنهجين: التحليلي والمقارن لنصوص القوانين العقابية الخاصة والقوانين المدنية في كل من مصر وفرنسا؛ وذلك من أجل التعرف على الكيفية التي عالجت فيها هذه الظاهرة، وفيما إذا كانت قد نجحت في مواجهتها أم لا، ونقارن الوضع لديها مع الوضع في العراق بظروفه وإمكاناته الأمنية والتقنية التي انعكست على تلك الظاهرة بشكل سلبي، وأدت إلى تزايد انتشارها، للتوصل فيما إذا كان بالإمكان تبني سياستها التشريعية سواء من ناحية صياغة السلوك التجريمي أم من ناحية القوة الرادعة للعقوبة، أم أن الوضع لدينا يتطلب تشددا أكثر في صياغة التشريع حتى يكفل الحد منها.

خطة البحث:

وللتعرف على هذه الظاهرة وللإجابة على التساؤلات المطروحة قسم البحث إلى ثلاثة مباحث: خصص المبحث الأول للتعريف بالظاهرة محل الدراسة ولبيان أهم الاختلافات بينها وبين التنمر التقليدي، وذلك في مطلبين أثنين، في حين تم تحديد المبحث الثاني لبيان المسؤولية الجزائية التي يمكن أن تترتب على ارتكابها، وما يتبع ذلك من ضرورة بيان أركان الجريمة وآثارها، ومن ثم قسم المبحث إلى مطلبين لتفصيل ذلك، في حين كان المبحث الثالث مخصصا لبيان المسؤولية المدنية من حيث أحكامها والآثار المترتبة عليها، وذلك في مطلبين أيضا، لننتهي بخاتمة تتضمن أهم ما توصلنا إليه من نتائج وتوصيات.

المبحث الأول: مفهوم التنمر الإلكتروني:

سنتطرق في هذا المبحث إلى مفهوم التنمر الإلكتروني، وسنقسمه إلى مطلبين نبين في الأول منهما تعريف التنمر الإلكتروني، ونتعرف في المطلب الثاني على التنمر التقليدي بصورة عامة، ثم نوضح أهم الاختلافات بينه وبين التنمر الإلكتروني، وذلك على النحو الآتي:

المطلب الأول: تعريف التنمر الإلكتروني

إن أول من صاغ موضوع التنمر الإلكتروني بشكل قانوني منذ العام (2001) هم: "نانسي ويلارد" وهي محامية أمريكية، و"بيل بيلسي" وهو مدرس في المدرسة الكندية، وقام بيلسي في العام (2008) بإنشاء موقع يخص موضوع التنمر الإلكتروني وهو (Cyberbulling.org)، ثم حددت نانسي مفهوم التنمر في العام (2003) بالقول أنه "لغة تشهيرية بسلوك متسلط متضمن تمييز أو مضايقة يكشف عن معلومات شخصية أو يحتوي على تعليقات مسيئة أو مبتذلة أو مهينة"، ولم تشر في هذا التعريف إلى استخدام شبكة الاتصال الحديثة في ارتكاب التنمر، ولكنها عدلت من مضمونه في العام (2007) وأضافت هذه الجزئية إليه، ثم تبعها بيلسي بوضع تعريف للتنمر في العام (2008) بالقول أنه "استخدام تقنيات المعلومات والاتصالات لدعم سلوك متعمد ومتكرر وعدائي من قبل فرد أو مجموعة من الأفراد بهدف إيذاء الآخرين" (غيبي، 2020، صفحة 97)

يعرّف الفقه التنمر الإلكتروني بأنه "مضايقات وتحرشات عن بعد باستخدام وسائل الاتصال الإلكتروني من طرف (متنمر) يقصد بها إيجاد جو نفسي لدى الضحية يتسم بالتهديد والقلق" (المكانين، الحياري، و يونس، 2018، صفحة 188)، وهو "الاعتداء على الآخرين والذي يمارس من خلال مواقع الصحف الإلكترونية. واستخدام كاميرات الموبايل، والبلوتوث، والتسجيلات الصوتية، بالإضافة لاختراق الخصوصيات عبر مواقع الإنترنت، بهدف إيقاع الأذى بالآخرين" (عبدالرحمن، 2018، صفحة 677)، ويعرف كذلك بأنه "ذلك السلوك الذي يهدف إلى إيذاء شخص آخر جسديا أو نفسيا من قبل شخص واحد أو عدة أشخاص وذلك بالقول أو الفعل للسيطرة على الضحية وإذلالها والحصول على مكتسبات غير شرعية منها وذلك باستخدام وسائل التواصل الاجتماعي" (بسيوني و الحربي، 2020، صفحة 130)، وهو أيضاً "السلوك المتكرر الذي يهدف إلى إيذاء شخص آخر جسديا أو لفظيا أو اجتماعيا أو جنسيا من قبل شخص واحد أو عدة أشخاص وذلك بالقول أو الفعل للسيطرة على الضحية وإذلالها والحصول على مكتسبات

غير شرعية" (العمار، 2016، صفحة 229)، ويعرف بأنه "التخويف والترهيب وما يشمل عليه من إساءة متعمدة والتي يتعرض لها الفرد من خلال استخدامه لخدمات شبكة الانترنت" (الزهراني، 2019، صفحة 161)، ويعرف أيضاً بأنه "سلوك تعسفي وعدواني بذيء ومهين يرتبط بنقص القدرة على التحكم في النفس وبالجهل وأذى كان قد وقع عليه" (الدسوقي، 2016، صفحة 10)

وعلى ضوء ما تقدم، يمكننا أن نعرف التنمر الإلكتروني بأنه كل سلوك عدواني متعمد ينال من حقوق الأفراد المعنوية، ويمارس عبر شبكة الاتصال الحديثة بتطبيقاتها المختلفة، وينشأ عنه ضررا معنويا وقد يصاحبه ضررا ماديا.

المطلب الثاني: تمييز التنمر الإلكتروني عن التقليدي

يعرف التنمر التقلي بأنه "سلوك تسبقه نية مبيتة وقصد متعمد لإيقاع الأذى والضرر بالضحية بهدف إخضاعه قسرا أو جبرا في إطار علاقة غير متكافئة ينجم عنها أضرار جسمية ونفسية وجنسية بطريقة متعمدة في مواقف تقتضي القوة والسيطرة على الضحية"، وهو أيضا "تعرض الضحية لسلوك متعمد متكرر من آخر أو آخرين يتضمن الإيذاء الجسدي واللفظي أو الإقصاء الاجتماعي أو التحرش الجنسي"، وهو يشتمل على أربع صور وهي التنمر اللفظي، والبدني والنفسي والجنسي والعرقي. (الخصاونة، 2020، صفحة 53)

يتميز التنمر التقليدي عن الإلكتروني بالمواجهة المباشرة بين المتنمر والمتنمر عليه، وهو على الخلاف من التنمر الإلكتروني الذي تكون فيه المواجهة غير مباشرة ويمارس عبر وسائل تقنية المعلومات الحديثة، إذ لا يتطلب أن يكون هنالك تقاربا مكانيا بينهما، ويعد هذا التنمر أكثر خطورة وأشد تأثيرا على الضحايا من التنمر التقليدي، بالنظر لسرعته في الانتشار، ولآثاره الترويعية على نفسية الضحية. (إبراهيم، 2020، صفحة 488)، والتنمر الإلكتروني في العادة يتحقق بصورتين: أما أن يكون تنمراً مباشرا، أو تنمراً غير مباشر، ويراد بالأول أن يوجه الإيذاء إلى شخصية الضحية مباشرة عبر الهاتف النقال أو بكتابة تعليقات على حساباته عبر مواقع التواصل الاجتماعي، في حين أن الثاني توجه الإساءة للضحية من خلال النشر على حسابات أصدقائه أو أقربائه أو بإرسال الرسائل إلى الهواتف الخاصة بهم، وهذا النوع يعد أكثر صعوبة من الأول بالنظر لعدم قدرة الضحية على إزالة تلك الإساءات من المواقع أو الهواتف لكونها خارجة عن صلاحياته. (كامل، 2018، الصفحات 29-30)

ويختلفان من حيث أن المتنمر الإلكتروني يكون من ناحية الشعور بالمجنى عليه أو التعاطف أو القلق أو الاهتمام به أقل مقارنة بالتنمر التقليدي، وهذا يرجع إلى طبيعة الوسائل الإلكترونية التي من شأنها أن تمكن المتنمر من التخفي والهرب دون أن يجازى على ما يلحقه بالمجنى عليه من ضرر نفسي أو عاطفي، ويختلفان كذلك من ناحية المهارة والمعرفة التكنولوجية التي يقتضي توافرها، فالمتنمر الإلكتروني يجب أن تتوافر فيه المهارة إلى الدرجة التي تمكنه من استخدام الوسائل الإلكترونية في إيذاء الآخرين والتخفي دون أن يتمكن أحد من التعرف عليه، (حسين، 2016، الصفحات 55-57) ومن الفروقات الأخرى صعوبة الهروب من التنمر الإلكتروني، فإذا كان بإمكان الضحية التخلص من التنمر التقليدي بمجرد العودة للمنزل، فأن التنمر الإلكتروني يبقى ملاحقا الضحية أينما ذهب لأنه يمكن أن يمارس عبر رسالة

ترسل من خلال الهاتف النقال أو تعليقات مسيئة ترتكب عبر مواقع التواصل الاجتماعي. (السويهري، 2019، صفحة 691)

ويختلفان كذلك من حيث توازن القوة والتكرار، فبالنسبة للأولى نجد أن التنمر التقليدي يكون أقل قوة من الإلكتروني نظرا لكونه يرتبط بالإمكانات الجسدية والنفسية للجاني بينما التنمر الإلكتروني يرتبط بقوة تكنولوجيا المعلومات وما تنطوي عليه من مزايا تعينه على أخفاء شخصيته وعدم الكشف عنها كما ذكرنا في أعلاه، أما بالنسبة للتكرار فأنه يتحقق في كلا الحالتين لكنه يكون أوسع انتشارا بالنسبة للتنمر الإلكتروني بالنظر لكون التكرار في التنمر التقليدي يقتصر على حالة المواجهة المباشرة بين الطرفين (المتنمر والضحية)، بينما يرتبط التكرار في التنمر الإلكتروني بالمزايا الواسعة لتكنولوجيا المعلومات. (درويش و الليثي، 2017، صفحة 206)، وتؤكد دراسات أن عامل القوة يتمثل في القدرة على التخفي وإخفاء المتنمر لهويته، وكلما نجح في ذلك كلما زاد تنمره مقارنة بالتنمر التقليدي. (حسين، 2016، صفحة 55)

ومن الاختلافات الأخرى أن التنمر الإلكتروني يرتكب في أي وقت كان على خلاف التقليدي، وأن عدد المشاهدين له أكثر بكثير من التنمر التقليدي، وأن ردود أفعالهم تختلف فقد يكونوا مساندين للمتنمر الإلكتروني من خلال مساهمتهم في إرسال ونشر ما يقوم به من عنف أو مساندين للضحية على خلاف التنمر التقليدي، وأن الدافع له قد يكون عدم قدرة المتنمر على إظهار قوته للآخرين على العكس من التنمر التقليدي الذي قد يرجع إلى الرغبة في إظهار المتنمر لقوته أمام الآخرين (عيد، 2019، الصفحات 578-579) ، ويختلفان أيضا من ناحية الاندفاع نحو الجريمة، فالمتنمر التقليدي لا يقدم على الفعل إلا بعد التفكير المتأني والتخطيط المكاني والزماني قبل التنفيذ، بينما يرتكب المتنمر الإلكتروني الفعل بشكل فوري دون تفكير أو حساب لتبعات أفعاله نظرا لسهولة ارتكابه وسرعته. (مقراني، 2018، صفحة 22)

المبحث الثاني: المسؤولية الجزائية المترتبة على التنمر الإلكتروني

سنتطرق في هذا المبحث إلى المسؤولية الجزائية من حيث بيان أركان جريمة التنمر الإلكتروني في ضوء كل من التشريع العقابي المصري والفرنسي، ثم نوضح الآثار التي رتبها المشرع في كل منهما عند تحقق تلك الأركان، وذلك في المطلبين الآتيين:

المطلب الأول: أركان جريمة التنمر الإلكتروني

تتكون الجريمة من ثلاثة أركان: الشرعي والمادي والمعنوي، ويقوم الأول على أساس وجود نص تجريمي يحرم ارتكاب الفعل وعدم وجود نص يبيحه، (الخلف و الشاوي، 2012، صفحة 151) وبالرجوع إلى التشريعات المقارنة نجد أن المشرع المصري نص على تجريم التنمر في قانون العقوبات النافذ بموجب المادة الأولى من التعديل الأخير رقم (189) لسنة 2020، إذ بمقتضاها تم إضافة نص جديد إلى القانون بالعدد (309/ مكرر ب)، ومن ثم فأن هذا النص يعد الأساس القانوني لتجريم التنمر، في حين نجد أن المشرع الفرنسي نص على تجريم التنمر في قانون العقوبات النافذ

بموجب المادة (222-33-2)، وقد جرى تعديل هذه المادة في عامي (2014 و2018)، وتبعا لهذا التعديل فأن المادة المذكورة تعد الأساس القانوني لتجريم التنمر الإلكتروني، أما بالنسبة للتشريع العراقي فأنه لم ينص على التنمر الإلكتروني في قانون العقوبات النافذ ولا القوانين العقابية المكملة له، وإذا ما ارتكبت أفعال تعد من جرائم التنمر الإلكتروني بحسب ما وصفه المشرع في التشريعات المقارنة، فأن الجاني لا يمكن أن يعاقب عن تنمر ، وإنما يعاقب بالوصف القانوني الذي يتناسب مع فعله، والذي تتحقق فيه الشروط التي يتطلبها القانون لتطبيق النص العقابي، كأن تطبق نصوص السب أو القذف، وذلك بالنظر لما يشكله فعله من عدوان على الحقوق محل الحماية القانونية ودون أن يخرج في ذلك عن مبدأ الشرعية، وإنما يعمل القاضي في هذه الحالة على تطبيق النصوص العقابية التقليدية التي تتضمن الحد الأدنى الذي يسمح بالتجريم دون تعارض مع المبدأ المذكور، وهذا يعد فراغا تشريعيا يفترض من المشرع أن يعمل على معالجته.

أما عن الركن المادي فهو السلوك الذي يصدر من المتنمر، وهو يشمل أي صورة من الصور الواردة في المادة (309) المذكورة أعلاه، وهي "قول أو استعراض قوة أو سيطرة للجاني أو استغلال ضعف للمجني عليه أو لحالة يعتقد الجاني أنها تسيء للمجني عليه كالجنس أو العرق أو الدين أو الأوصاف البدنية أو الحالة الصحية أو العقلية أو المستوى الاجتماعي". وتعد الصورة الأولى التنمر القولي أو اللفظي من أكثر الصور انتشارا بالنسبة للتنمر التقليدي، وهي تشمل كل تعدي ينطوي على إطلاق عبارات تهدف إلى السخرية أو التقليل من شأن الضحية أو انتقادها، ويستوي في ذلك أن يكون القول جملة أو جزءا منها أو لفظا أو جزءا منه طالما أن له دلالة تمس بالضحية، أما بالنسبة للتنمر الإلكتروني فأن الركن المادي له يرتكب عبر استخدام الوسائل الرقمية كالهواتف والحواسيب والأجهزة الإلكترونية الحديثة الأخرى، وهو سلوك عدائي متكرر يهدف إلى تخويف الضحية واستفزازها أو إحراجها، كقيام المتنمر بنشر صور شخصية من شأنها إحراج الضحية، أو مقاطع فيديوية تم تصميمها بشكل قاصدا بها تشويه سمعتها أو إيذائها بأي طريقة كانت، ويدخل ضمن الركن المادي أيضا كل تعليق غير لائق من الناحية الاجتماعية والأخلاقية سواء أكان على صورة خاصة بالضحية أم بمقالة أم بمقاطع فيديوية تم تداولها عبر شبكات الاتصال الحديثة، أو التهكم على شخصية الضحية، أو التعديل على صور حقيقية ونشرها بحيث يترتب عليها إحراجا للضحية، أو نشر معلومات كاذبة بهدف الإساءة للضحية أو تشويه سمعتها، أو استبعادها إلكترونيا ونبذها، أو المشاركة الإلكترونية لكل ما من شأنه إيذاء الآخرين، (المرى، 2021، صفحة 14) وغيرها من الصور التي يمكن أن تصدر عن المتنمر وتلحق الأذى بالمتنمر عليهم، ويكون منطويا عليها المعاني الواردة في المادة المذكورة في أعلاه وترتكب بوسيلة إلكترونية.

أما في فرنسا فنجد أن الركن المادي لجريمة التنمر يتمثل في ثلاثة صور، أحداهما التنمر الذي يمارس ضد شخص آخر من خلال مضايقته بكلمات أو سلوكيات متكررة من شأنها أن تؤدي إلى المساس بحقوقه وكرامته وتسبب التدهور في ظروف عمله وإلحاق أضرار بصحته البدنية والعقلية، أو تمس بمستقبل مهنته، وهذه الصورة وردت في المادة (40) من التعديل ذي العدد (873) للعام 2014 الذي طرأ على المادة (222-33-2) من قانون العقوبات الفرنسي، وثانيهما التنمر الذي يقع بين الأزواج أو الشركاء، وهو يتحقق بالمضايقة الكلامية أو السلوكية المتكررة ضد الزوج أو الشريك والتي ينتج عنها تدهورا في الظروف المعيشية أو الصحة العقلية أم البدنية، سواء ترتب عليها عجز كلي عن

ممارسة العمل أم لم يترتب، وقد فرق المشرع في العقوبة بحسب طول مدة العجز وهو ما سنبينه عند الحديث عن العقوبة، ووردت هذه الصورة في المادة (13) من التعديل ذي العدد (703) لسنة 2018 بتاريخ 2018/8/3 الذي طرأ على المادة (222-33-2-1)، وثالثهما تشمل المضايقة الكلامية أو السلوكية المتكررة التي ترتكب من عدة جناة (تعدد المتنمرون) متى ما نشأ عن فعلهم تدهور الظروف المعيشية والصحية سواء العقلية منها أم البدنية للمتنمر عليه، ويستوي أن ينشأ عن هذا الفعل عجز كلي عن ممارسة عمله لمدة تساوي أو تقل عن (8) أيام أو لم يترتب، وتتحقق الجريمة في هذه الصورة **أما** بارتكاب الفعل من قبل عدة أشخاص تدخلوا بالفعل من خلال الاتفاق بينهم أو التحريض من احدهم، ويكفي أن يرتكب كل منهم فعل دون أن يكون هنالك تكرار من قبل كل منهم، **وإما** أن يرتكب من عدة أشخاص على الضحية ذاتها وعلى التوالي، وهم يعلمون أن هذه الأفعال تتسم بالتكرار حتى وأن لم يكن هنالك أتفاق بينهم، وأشارت إلى هذه الصورة المادة (11) من تعديل 2018 المشار إليه في أعلاه. (غيبي، 2020، الصفحات 107-108)

ومن أكثر الأساليب التكنولوجية التي استخدمت في ارتكاب سلوك التنمر ولاسيما بين طلاب الدراسة الثانوية (درويش و الليثي، 2017، صفحة 207) هي: المكالمات الصوتية التي تهدف إلقاء الروع بنفس الضحية سواء أكانت عبر الويب أم الهواتف، الرسائل النصية التي تتضمن تهديدا بافتعال الفضائح أو إفشاء الإسرار، الصور ومقاطع الفيديو الخاصة بالحياة الشخصية للضحية والتي يستولي عليها المتنمر وينشرها للغير، البريد الإلكتروني وفيه يرسل المتنمر رسالة إلى الضحية، وبمجرد فتحها يستولي على حساب الضحية دون علمه، ومن ثم يطلع على مراسلاته ومحادثاته الخاصة، وقد يجري بعض التصرفات التي من شأنها التسبب في مشاكل اجتماعية له وتوقعه في الحرج. (النجار، 2020، الصفحات 143-144) مواقع الدردشة ومن خلالها يتحدث المتنمر مع الضحية عبر حسابات وهمية ويحاول إلحاق الأذى به أو الاستيلاء على حسابه ونشر صور أو روابط مسيئة للضحية، مواقع الويب الخداعية وهي مواقع ينشر من خلالها أخبار تكون لافتة للانتباه وبمجرد الدخول على هذه المواقع يتمكن المتنمر من النشر على الصفحة الشخصية للضحية، وقد تكون في هذه المواقع تطبيقات تسمح للمتنمر بفتح الكاميرا وتصوير الضحية وتخويفه بصورة متكررة، وتؤكد الدراسات أن التنمر أما أن يقع بواسطة الانترنت من خلال تطبيقاته المختلفة، وأما من خلال الهواتف النقالة، وقد بينت إحدى الدراسات التي أجريت على (336) من الطلاب، أن نسبة (27.4%) منهم تعرض للتنمر عبر الانترنت، ونسبة (57.2%) تعرض للتنمر عبر الهاتف. (درويش و الليثي، 2017، صفحة 207)

أن تحقق السلوك الإجرامي لا يكفي لقيام جريمة التنمر وإنما لابد من أن يترتب عليه أثره، وهو تحقق النتيجة الإجرامية، والأخيرة تتحقق إذا أدى السلوك إلى إقصائه من محيطه أو حط من قدره، أو أساء إليه بمعتقداته الدينية أم بعرقه أم بجنسه أم بشكله أم بحالته الصحية والعقلية، أو بالمستوى الاجتماعي له، أو أدى السلوك إلى تخويف الضحية فعلا، وتفصل محكمة الموضوع في مدى تحقق النتيجة من عدمها باعتبارها مسألة موضوعية خاضعة لسلطتها التقديرية. (المرى، 2021، صفحة 15)

الركن المعنوي يعد التنمر جريمة عمدية، تقصد فيها الجاني السلوك والنتيجة معا، وهي من الجرائم التي لا تكتفِ بالقصد العام الذي يقوم على العلم والإرادة فقط، (أي العلم بأن فعله من شأنه المساس بالضحية ومع ذلك

تتجه إرادته إلى إتيان السلوك المادي للتنمر)، وإنما يتطلب توافر القصد الخاص أي نية تحقق غاية معينة إلى جانب القصد العام، (المرى، 2021، صفحة 15) وهذا القصد عبرت عنه المادة (309) المذكورة في التشريع المصري، بالقول: "... بقصد تخويفه أو وضعه موضع السخرية أو الحط من شأنه أو إقصائه من محيطه الاجتماعي..."

المطلب الثاني: آثار جريمة التنمر الإلكتروني

يترتب على ارتكاب جريمة التنمر الإلكتروني عقوبات جزائية تراوحت بين العقوبات السالبة للحرية والعقوبات المالية، إذ حددها المشرع المصري بالحبس وقيد حدها الأدنى بما لا يقل عن (6) أشهر، أو الغرامة المقيدة بين حدين أدنى لا يقل عن (10000) جنيه، وأعلى لا يتعدى (30000) جنيه، أو كلاهما دون أن يخل ذلك بتطبيق أي عقوبة تكون أشد واردة في أي قانون عقابي آخر، وتشدد المشرع المصري بالنسبة للجريمة المرتكبة من قبل أكثر من شخص، أو أن الجاني كان ذا صفة كأن يكون أصل للضحية أو من المتولين تربيته أو له سلطة عليه، أو كان الأخير قد سلم إليه بموجب القانون، أو حكم القضاء، أو كان الضحية يعمل خادما لدى مرتكب الفعل، وتكون العقوبة في هذا الحالة الحبس المقيد بما لا يقل عن (1) سنة، والغرامة المقيدة بما لا تقل عن (20000) جنيه ولا تتعدى (100000) جنيه، أو إحداهما، وإذ تمت الجريمة باجتماع الظرفين فأن أثر ذلك يتمثل بمضاعفة الحد الأدنى للعقوبة، وإذا حصل العود فأن الجريمة تضاعف في كل من حديها الأدنى والأعلى. (تعديل قانون العقوبات المصري، 2020، المادة (1)).

وبالنظر لخطورة جريمة التنمر الإلكتروني وما يترتب عليها من أضرار نفسية كبيرة على الضحية محل الجريمة، نجد أن المشرع المصري أقدم على تعديل القانون الخاص بحقوق الأشخاص ذوي الإعاقة رقم (10) لسنة 2018، وإضافة نص يعاقب على التنمر الذي يمارس ضد هذه الفئة من الأفراد بعقوبات أشد من العقوبات الواردة في القانون أعلاه، إذ قرر إضافة مادة عقابية بالرقم (50 مكرر) تقضي بمعاقبة المتنمر بالحبس المقيد بما لا يقل عن (2) سنة والغرامة المقيدة بما لا يقل عن (50000) جنيه ولا يتعدى (100000) جنيه، أو إحداهما لكل من يتنمر على ذوي الإعاقة، وقرر رفع الحد الأدنى للحبس إلى (3) سنوات والأعلى إلى (5) سنوات، والحد الأدنى للغرامة إلى (100000) جنيه والحد الأعلى إلى (200000) جنيه مع بقاء حق الخيار للقاضي بين تطبيق كلا العقوبتين أو أحداهما إذا توافر ظرفا من الظروف المشددة المشار إليها سابقا في المادة (309/ مكرر ب) مع تطبيق باقي الأحكام المذكورة فيها ذاتها عند تحقق شروطها. (تعديل قانون حقوق الأشخاص ذوي الإعاقة، 2021، المادة (1))

أما عن آثار الجريمة في القانون الفرنسي فأنها تراوحت بين الحبس والسجن إضافة للعقوبات المالية، إذا فرق المشرع الفرنسي بين صور التنمر الثلاثة من حيث العقوبة ولم يساوي بينها، فالصورة الأولى المشار إليها في المادة (40) يعاقب عليها بالحبس لسنتين وغرامة (30000) يورو، بينما جعل عقوبة الصورة الثانية أشد إذ جعل الحبس لـ (3) سنوات مع غرامة تقدر بـ(45000) يورو، وتشدد في العقوبة إلى السجن لخمس سنين وغرامة (75000) يورو، إذ نشأ عن الفعل عجز كلي عن ممارسة العمل لمدة تزيد عن (8) أيام، أو إذا ارتكبت الجريمة أمام قاصر، أو تمت من قبل زوج أو شريك سابقين، أما عن الصورة الأخيرة فقد جعل المشرع عقوبتها الحبس لسنة واحدة مع الغرامة التي تقدر بـ (15000) يورو، وتشدد العقوبة لمدة سنتين حبس و(30000) يورو غرامة، أذا توافرت أحدى الظروف المشددة، وهي

حصول عجز تام عن العمل لأكثر من (8) أيام، أو كان الضحية قاصرا (15 سنة)، أو كان الضحية في حالة ضعف واضحة أو معروفة من قبل المتنمر كما لو كان مريضا أو عاجزا أو صغير السن أو معاق جسديا أم عقليا أو كانت امرأة حاملا، أو ارتكبت عبر خدمات الاتصال العامة عبر شبكة الانترنت أو وسيط رقمي، أو تمت بحضور قاصر، وإذا اجتمع اثنين من الظروف المذكورة فأن العقوبة تشدد إلى الثلاث سنوات والغرامة التي تبلغ (45000) يورو، ولم تكتفِ فرنسا في التصدي للتنمر الإلكتروني بهذه العقوبات الرادعة لخطر الجريمة، وإنما تعمل بعض اللجان فيها ومنها "اللجنة الوطنية للمعلومات والحريات" و"المجلس السمعي البصري الأعلى" على توعية الجمهور وتثقيفه من خطر هذه الجريمة، وهي إجراءات وقائية سابقة على وقوعها وتستهدف الحد منها. (غيبي، 2020، الصفحات 106-108)

إما عن موقف المشرع العراقي فقد ذكرنا سابقا أنه لا يوجد نص يجرم التنمر الإلكتروني، وأن هذه الأفعال إذا ما ارتكبت فأن القاضي يطبق عليها نصوص التهديد أو القذف والسب إذا ما تحققت شروطها، وبناء عليه فأن العقوبات تختلف بحسب الفعل المرتكب وبحسب تكييف القاضي له، فإذا كييف الفعل على أنه تهديد إذا تحققت شروطه فيخضع الجاني لعقوبات جريمة التهديد التي تتراوح بين السجن والحبس، وإذا كييف الفعل أنه سب أو قذف إذا تحقق شروطه، فأنه يخضع لعقوبات هذه الجرائم المنصوص عليها في القانون وهي الحبس المطلق أو المقيد والغرامة أو إحداهما.

وعلى ضوء ما تقدم ذكره، فأن الوضع في العراق في ظل غياب التشريعات العقابية المنظمة لهذا الموضوع، يظهر لنا مدى الحاجة إلى التدخل بسن قوانين تكفل الحماية الكافية للأفراد من الاعتداءات المذكورة، خاصة وأنها منتشرة فعليا وبشكل كبير عبر مواقع التواصل الاجتماعي، ومن خلال الإطلاع على التنظيم التشريعي لمجابهة هذه الظاهرة في كل من مصر وفرنسا، نستطيع القول إن كلا الدولتين سعت في قوانينها العقابية التي عالجت الموضوع إلى إتباع سياسية تشريعية مرنة في تحديدها للسلوك الإجرامي المكون للجريمة، ففي القانون المصري نجد أنه ذكر في المادة (309) سالفة الذكر عدة صور للسلوك الإجرامي ولم يقصره على صورة واحدة، كذلك الفرنسي الذي نص على ثلاث صور للتنمر، وهي سياسة محمودة كون الظاهرة لا زالت حديثة ولم تتضح معالمها بالشكل الدقيق، وأن تنويع صور السلوك يعني أن المشرع تصدى لأكبر قدر من الخطورة لهذه الظاهرة، ومن ثم فأن توسيع صور السلوك الإجرامي انعكس إيجابا على قوة التشريع بزيادة فاعليته في التصدي للتنمر الإلكتروني، ونأمل من المشرع العراقي أن يتبنى هذه السياسة في صياغته لنصوصه العقابية للحد من هذه الظاهرة، أما بالنسبة لسياسة العقاب التي انتهجتها فأن لم تكن بمستوى سياسة التجريم وإنما كانت أقل صرامة، إذ أنها جعلت عقوباتها الحبس المقيد في غالبية حالات ارتكابها، وهي عقوبة لا نعتقد أنها يمكن أن تحقق غرضها في الردع، خاصة وأن طريقة ارتكاب هذه الجريمة تحمل مغريات كثيرة للجناة تدفعهم نحو ارتكابها، ومنها سهولة اقتراف الفعل والقدرة على التخفي، وأمام هذه المغريات فأن سياسية العقاب يجب أن تكون على درجة من الشدة لأجل أن تضمن ردع الجناة، لذا نأمل من مشرعنا أن يتبنى سياسة عقابية أكثر شدة مما تبنته الدول المقارنة، لضمان السيطرة على هذه الظاهرة والحد منها.

المبحث الثالث: المسؤولية المدنية المترتبة على التنمر الإلكتروني

سنبين في هذا المبحث أحكام المسؤولية المدنية التي يمكن أن تترتب على ارتكاب جريمة التنمر الإلكتروني وآثارها، وسنقسمه إلى مطلبين نوضح في الأول منهما مفهوم المسؤولية المدنية وأركانها من خطأ وضرر وعلاقة سببية، وفي الثاني نوضح التعويض كأثر لهذه المسؤولية سواء أكان عيني أم نقدي، وذلك على النحو الآتي:

المطلب الأول: أحكام المسؤولية المدنية المترتبة على التنمر الإلكتروني

تعرف المسؤولية المدنية بأنها نظام الغاية منه تعويض الأضرار التي تلحق بالغير من جراء أفعال غير مشروعة أو ضارة تصدر من شخص ما ولا تتضمن معنى الزجر أو العقاب وإنما فقط إزالة ما نشأ عن الفعل من أضرار، (البيات، د.س، صفحة 53) وهي أيضا كل إخلال بالتزام ينشأ عنه ضررا للغير ويوجب على صاحبه تعويض ذلك الضرر بإزالة آثاره. (عبدالرؤوف، 2019، صفحة 418)

وبالرجوع إلى الأساس القانوني لهذه المسؤولية نجد أن التشريعات أخذت بها في نصوصها المدنية، ومنها المشرع العراقي الذي نص على هذه المسؤولية في المادتين (202 و204)، وبموجب هذان النصان فأن الأفعال الضارة بالغير ترتب على صاحبها مسؤولية تقصيرية، أساسها الإخلال بالتزام قانوني، سواء أكانت هذه الأفعال ضد النفس كما في جرائم القتل والضرب والجرح وغيرها أو لم تكن ضد النفس ولكن أصابت الغير بضرر، (القانون المدني العراقي المعدل، 1951)، وفي مصر نص عليها المشرع في المادة (163) التي أشارت إلى أنه كل شخص يرتكب خطأ يترتب عليه ضررا لآخر فأنه يلتزم بالتعويض (القانون المدني المصري المعدل، 1948)، وفي فرنسا نص عليها المشرع في المادة (1382) التي أشارت إلى إلزام كل من يخطئ بتعويض الضرر الذي يلحقه بالغير، ويشترط لتحقق هذه المسؤولية توافر ثلاثة أركان هي: الخطأ والضرر والعلاقة السببية، وبدونها لا وجود للمسؤولية التقصيرية.

ويراد بالخطأ أو ما يسمى بالفعل غير المشروع الإخلال بما يفرضه القانون من أوامر تلزم الفرد بعدم إلحاق الضرر بالغير، ويعرف أيضا بأنه الإخلال الواعي بالواجبات القانونية، وهو كذلك الإخلال بالواجبات العامة أو الخاصة التي يفرضها القانون على الأفراد داخل الجماعة وتلزمهم باحترام حقوق الغير وحرياتهم وعدم التعدي عليها ، وهذا الخطأ يقوم على عنصرين أحدهما تعدي حدود الواجبات التي يفرضها القانون، وثانيهما هو أن يتوافر الإدراك لدى المتعدي، فأن ثبت العكس لا يتحمل المسؤولية، فالأخيرة لا تقوم بحق المتعدي إلا إذا توفر كلا عنصري الخطأ. (الدليمي، 2020، الصفحات 60-63)

أن تحقق الخطأ وحده لا يكفي وإنما لابد من أن يترتب عليه مساس بمصلحة أو حق مشروع للضحية سواء أصاب جسده أم شرفه أم حريته أم عاطفته وغيرها، والضرر بصورة عامة أما أن يكون ماديا يخل بالمصالح المالية للضحية أو بصحته أو سلامة بدنه أو أي حق من حقوقه الشخصية طالما ترتب عليها خسائر في ذمته المالية، أو يكون أدبيا، والضرر الأدبي يصيب الضحية في عاطفته أو شرفه أو اعتباره أو سمعته ويسبب له ألما معنويا فقط، وأن تكون

هنالك رابطة سببية بين كل من الخطأ الصادر من الجاني والضرر الذي يلحق بالضحية. (الدليمي، 2020، الصفحات 81-85)

وبالرجوع إلى موضوع دراستنا فأن المسؤولية المدنية متحققة بأركانها الثلاثة، إذ بمجرد أن يرتكب المتنمر الجريمة بأي صورة من صور السلوك الإجرامي المشار إليها سابقا، يتحقق الركن الأول وهو الخطأ ويتحقق تبعا له ركن الضرر باعتباره أثرا للسلوك، وهو ضررا أدبيا يسبب ألما نفسيا للضحية، وذلك بحكم أن ما ينشر على مواقع التواصل الاجتماعي من إساءات من شأنها أن تنال من الاعتبار الأدبي للضحية دون أن تمس كيانه المادي، وقد يؤدي هذا الضرر الأدبي إلى ضرر مادي متى ما ترتب على الجريمة خسائر مادية أيا كان نوعها، كأن يمتد ضرر التنمر إلى مجال عمله فيخسر وظيفته نتيجة الإساءات التي وجهت إليه وغيرها، وتبعا لما ذكر فأن المسؤولية المدنية بحق الجاني تقوم مع المسؤولية الجزائية، لا بل أن المسؤولية المدنية تبقى قائما حتى لو انتفت المسؤولية الجزائية بسبب وجود مانع من موانع المسؤولية الجزائية الواردة في قانون العقوبات.

المطلب الثاني: آثار المسؤولية المدنية المترتبة على التنمر الالكتروني

أن الأثر المترتب على المسؤولية المدنية هو التعويض، وهو على نوعين: أما أن يكون بإعادة الحال إلى ما كان عليه إذا أمكن ذلك، وهذه الصورة من التعويض لا تتحقق في نطاق المسؤولية التقصيرية إلا في حالات نادرة، وذلك بالنظر لكون الضرر لا يمكن أن يزال فيها عينا، ومع ذلك فأن بالإمكان تصور تحققه، فإذا كان الضرر أدبيا وناشئا عن نشر منشورات مسيئة عبر مواقع التواصل الاجتماعي فأنه يمكن إزالة هذا الضرر عينا من خلال حذف المنشور وإلزام صاحبه بنشر تكذيب لمحتوى منشوره السابق، وقد يكون التعويض في صورة اعتذار ينشر في نفس الموقع الذي تم النشر فيه، وقد أقر كل من التشريع والقضاء بالتعويض العيني كوسيلة لجبر الضرر، إذ اقر به المشرع العراقي في المادة (2/209) والمشرع المصري في المادة (2/171) من قوانينهما المدنية، وأشارت محكمة النقض المصرية في حكم لها بأن التعويض العيني يتم من خلال العمل على إزالة الأضرار وأعادت الوضع إلى ما كان قبل اقتراف الخطأ، وأشارت محكمة النقض الفرنسية أن التعويض العيني هو إحدى طرق التعويض عن الإضرار (مهدي، 2020، الصفحات 87-90) .

وإما أن يكون بالتخفيف من شدة الضرر من خلال التعويض النقدي، (الزبيدي، 2018، الصفحات 418-419)، وتعد النقود أفضل وسيلة لتعويض الأضرار المادية منها والأدبية، ويلجأ إليه عند تعذر التعويض العيني، ففي الحالات التي يكون فيها الضرر ناشئا عن نشر خبر عن شخص يعمل بشركة ما وترتب على نشره خسارة الضحية لعمله، فأن التعويض العيني لا يجدِ نفعا ومن ثم فأنه يجب أن يصار إلى التعويض النقدي، ومن الأمثلة على التعويض النقدي مصادقة محكمة التمييز الاتحادية على حكم محكمة الموضوع الذي قضى بإلزام المدعى عليه بالتعويض النقدي عن أفعاله المسيئة لسمعة الضحية، إذ قام بنشر صور ومقاطع فيديوية تضمنت إساءة للضحية على الصفحة الشخصية للفيس الخاص به، وبشكل يتناف مع ما تقضي به حرية الرأي والتعبير، وقد استندت المحكمة على تقارير الخبراء في تحديد مبلغ التعويض بـ(3) ملايين دينار. (مهدي، 2020، الصفحات 91-92)

وبالنسبة لموضوع دراستنا جريمة التنمر الإلكتروني، فأننا نعتقد وبتواضع أن أفضل وسيلة لتعويض أضرار هذه الجريمة هو التعويض النقدي وبمبالغ مالية كبيرة لأجل أن تكون رادعة للجناة، فضلا عن إلزامه بحذف كافة المنشورات النصية والفيديوية المسيئة للضحية مع تقديم اعتذار ينشر في الموقع ذاته الذي ارتكبت فيه الجريمة.

خاتمة:

وبعد أن أوضحنا كل ما يتعلق بموضوع البحث توصلنا إلى النتائج والمقترحات الآتية:

أولا-النتائج:

- ✓ إن ظاهرة التنمر الإلكتروني منتشرة بشكل واسع وترتكب من قبل المتنمرين عبر مواقع التواصل الاجتماعي، ولكن القضاء العراقي لا يعاقب علها تحت هذا الوصف وإنما كجرائم تقليدية مثل السب والقذف أن تحققت شروطها، وأن لم تتحقق فأنها تبقى أفعالا مباحة لا عقاب عليها رغم ما تنطويه من تعد على حقوق الأفراد وحرياتهم، ولا يخفى أن هذا الإجراء (إدخالها ضمن الجرائم التقليدية) لا يمكن أن يحد من هذه الظاهرة المتنامية، كون النصوص الواردة في قانون العقوبات النافذ وضعت لمعالجة الاعتداءات التي ترتكب وجها لوجه وهي أقل ضرر من هذه الظواهر.
- ✓ أن ظاهرة التنمر الإلكتروني تسبب أضرار معنوية في الغالب الأعم من حالات ارتكابها، وأن كانت في بعض صور ارتكابها تؤدي إلى أضرار مادية بجانب الأضرار المعنوية وهو ما يجعلها أبلغ تأثيرا على الضحايا من الجرائم التقليدية بما فيها التنمر التقليدي.
- ✓ أن السياسية التشريعية التي اتبعتها الدول المقارنة من ناحية التجريم جعلت السلوك الإجرامي شاملا لعدد كبير من التجاوزات التي ترتكب عبر مواقع التواصل الاجتماعي، وهو اتجاه يتوافق مع ما تقتضي به طبيعة هذه الظاهرة المتنامية.
- ✓ 4أن المواجهة العقابية لهذه الظاهرة اقتصرت على الحبس من العقوبات السالبة للحرية ولم تصل إلى عقوبة السجن حتى مع وجود الظروف المشددة إلا في حالات نادر، ومن ثم فأن سياسة العقاب لم تكن بالمستوى الفاعل مقارنة بسياسة التجريم.
- ✓ أن التعويض عن أضرار الجريمة لا يمكن أن يحقق الغاية منه إلا إذا اقترن التعويض النقدي بالعيني، كون المبالغ المالية لا يمكن أن تجبر الضرر طالما أن المنشورات لا تزال متداولة عبر مواقع التواصل الاجتماعي، وهذا يتطلب أن يُلزم الجاني بحذف المنشور مع نشر اعتذار في المواقع ذاتها.

ثانيا-المقترحات:

- ✓ ضرورة توجه المشرع نحو صياغة نصوص جزائية رادعة للحد من هذه الظاهرة، وذلك بالإسراع في الموافقة على مشروع قانون جرائم المعلوماتية الذي قدم منذ العام 2011، بعد أن يضاف له مادة تعاقب على التنمر الإلكتروني، وأن يساير في صياغة نصه التجريمي التشريعات المقارنة بأن يمسح بشموله لأكبر عدد ممكن من التجاوزات الإلكترونية، وأن يحدد له عقوبات أكثر شدة مما أخذت به تلك التشريعات لضمان تحقيق قوة رادعة لنصوصه، وأن يشمل

بعقوباته الحبس والسجن فضلا عن العقوبات المالية وبحسب الفعل المرتكب، مع تشديد العقوبة عند توافر ظروفا تستدعي ذلك.

- ✓ أنشاء هيئات أو لجان متخصصة مهمتها الأساسية تثقيف وتوعية الجمهور حول ظاهرة التنمر وكيفية مواجهتها، وذلك من خلال إقامة الورش والندوات، فضلا عن استثمار مواقع التواصل الاجتماعي لنشر تلك البرامج التوعوية سواء أكانت على شكل كتيبات أم صور أم مقاطع فيديوية توضح مخاطر هذه الجريمة، وما يمكن أن تسببه من أضرار، وكيف يمكن التخلص منها.
- ✓ إنشاء شرطة إلكترونية تكون متخصصة برصد ومتابعة الجرائم الإلكترونية حصرا، ويتم تدريبها وتجهيزها بأحدث الوسائل التقنية لملاحقة مرتكبي هذه الجرائم، مع ضرورة تخصيص خط ساخن للتبليغ عنها، وتيسير إجراءات التواصل مع المخبرين وإبقاء شخصياتهم مجهولة.

قائمة المراجع:

1) القانون المدني العراقي المعدل. (1951). رقم (40).

2) القانون المدني المصري المعدل. (1948). رقم (131).

3) أمل يوسف عبدالله العمار. (2016). التنمر الإلكتروني وعلاقته بأدمان الإنترنت في ضوء بعض المتغيرات الديمغرافية لدى طلاب وطالبات التعليم التطبيقي بدولة الكويت. (3 الجزء) مجلة البحث العلمي في التربية. (العدد 17).

4) بهاء المرى. (2021). التنمر والجرائم المشتبهة. المنصورة: دار الاهرام.

5) تعديل قانون العقوبات المصري. (2020). رقم 189.

6) تعديل قانون حقوق الأشخاص ذوي الإعاقة المصري. (2021). رقم (156).

7) حسنية حسين عبدالرحمن. (يناير، 2018). تصور مقترح للتغلب على التنمر الإلكتروني في مدارس التعليم الأساسي بجمهورية مصر العربية على ضوء خبرات كل من استراليا وفنلندا والولايات المتحدة الأمريكية. (2، الجزء) مجلة التربية. (العدد 177).

8) رشا عادل عبدالعزيز إبراهيم. (يناير، 2020). فعالية برنامج إرشادي معرفي سلوكي في استخدام استراتيجيات مواجهة التنمر الإلكتروني لدى طلاب المرحلة الثانوية. (30 المجلد) المجلة المصرية للدراسات النفسية. (العدد106).

9) رمضان عاشور حسين. (سبتمبر، 2016). البيئة العاملية لمقياس التنمر الإلكتروني كما تدركها الضحية لدى عينة من المراهقين. المجلة العربية لدراسات وبحوث العلوم التربوية والإنسانية. (العدد 4).

10) سحر فؤاد مجيد النجار. (2020). جريمة التنمر الإلكتروني(دراسة في القانون العراقي والأمريكي). (المجلد 11) المجلة الأكاديمية للبحث القانوني. (العدد 4) .

11) سعود ساطي السويهري. (يناير، 2019). الحد من سلوكيات التنمر الإلكتروني والتأثيرات السلبية للسيبرانية على الشخصية الإنسانية. (المجلد 73) مجلة كلية التربية (العدد (1)).

12) سوزان بنت صدقة بسيوني، و ملاك بنت علي الحربي. (30 مارس، 2020). التنمر الإلكتروني وعلاقته بالوحدة النفسية لدى طالبات كلية التربية بجامعة أم القرى. (4المجلد) مجلة العلوم التربوية والنفسية. (العدد 12).

13) صخر أحمد الخصاونة. (2020). مدى كفاية التشريعات الإلكترونية للحد من التنمر الإلكتروني-دراسة في التشريع الأردني. المجلة الدولة للدراسات القانونية والفقهية المقارنة.(العدد 2) .

14) ضياء مسلم عبد الامير غيبي. (2020). الحماية القانونية من التنمر الإلكتروني بجائحة كورونا. مجلة الكوفة.(العدد 2/47) .

15) عامر حمد غضبان عويد الدليمي. (حزيران، 2020). مسؤولية القاضي المدنية في التشريع العراقي. رسالة ماجستير . جامعة الشرق الأوسط.

16) علي حسين الخلف، و سلطان الشاوي. (2012). المبادئ العامة في قانون العقوبات (المجلد د.ط). بغداد: مكتبة السنهوري.

17) عمر محمد محمد أحمد درويش، و أحمد حسن محمد الليثي. (أكتوبر، 2017). فاعلية بيئة تعلم معرفي / سلوكي قائمة على المفضلات الاجتماعية في تنمية استراتيجيات مواجهة التنمر الإلكتروني لطلاب المرحلة الثانوية. مجلة العلوم التربوية (ج (1)). (العدد 4).

18) مباركة مقراني. (2018). التنمر الإلكتروني وعلاقته بالقلق الاجتماعي. رسالة ماجستير . كلية العلوم الإنسانية والإجتماعية، جامعة قاصدي مرباح ورقلة.

19) مجدي محمد الدسوقي. (2016). مقياس السلوك التنمري للأطفال والمراهقين (المجلد د ط). القاهرة: دار العلوم.

20) محمد حاتم البيات. (د.س). النظرية العامة للإلتزام (مصادر الإلتزام). منشورات جامعة دمشق.

21) محمد رفعت عبدالرؤوف. (يناير، 2019). تقدير التعويض عن الخطأ. مجلة بحوث الشرق الأوسط ، (العدد 48).

22) محمود عمر أحمد عيد. (سبتمبر، 2019). واقع التنمر الإلكتروني على شبكات التواصل الإجتماعي بين طلاب الجامعة. المجلة التربوية.(65) .

23) محمود كامل محمد كامل. (2018). التنمر الإلكتروني وتقدير الذات لدى عينة من الطلاب المراهقين الصم وضعاف السمع. رسالة ماجستير . مصر: جامعة طنطا، كلية التربية.

24) مروة صالح مهدي. (حزيران، 2020). المسؤولية المدنية عن النشر الإلكتروني. رسالة ماجستير . جامعة الشرق الأوسط.

25) نبراس زاهر الزيدي. (2018). المسؤولية المدنية الناشئة عن إخلال الغير بالعقد. مجلة المحقق الحلي للعلوم القانونية والسياسية. (العدد 1).

26) نورة مسفر عطية الغبيشي الزهراني. (يوليو، 2019). التوافق الأسري وعلاقته بالتنمر الإلكتروني لدى الأبناء. مجلة الفنون والأدب وعلوم الانسانيات والاجتماع . (العدد 40).

27) هشام عبدالفتاح المكانين، غالب محمد الحياري، و نجاتي أحمد يونس. (يناير، 2018). التنمر الإلكتروني لدى عينة من الطلبة المضطربين سلوكيا وانفعاليا في مدينة الزرقاء. (12المجلد) مجلة الدراسات التربوية والنفسية -جامعة السلطان قابوس. (العدد 1).

دور النيابة العامة في التصدي للجرائم المعلوماتية على ضوء التشريع المغربي

The role of public persecution in comforting cyber crime in lights of the Moroccan legislation.

ط.د.بيشا حسان/ جامعة الحسن الأول، سطات/ المغرب

Dr.Baicha Hassan/ University Hassan 1, Settat / Morocco

ملخص الدراسة:

في كنف التطور التكنولوجي الحديث لشبكة المعلومات وثورة الاتصالات والحواسب الألية والهواتف الذكية، وفي ظل العولة وما أفرزته من كسر للحدود، ظهر الجريمة المعلوماتية كنمط جديد من الإجرام خلف آثار سلبية على المستوى الاجتماعي والاقتصادي والأمني، الأمر الذي دفع ضرورة التدخل من خطر هذه الظاهرة.

والنيابة العامة باعتبارها جزء من السلطة القضائية تعمل على تأمين الاستعمال الأمثل للتكنولوجيا الرقمية، وحماية الاقتصاد الرقمي عبر تطوير آليات رصد الجرائم الإلكترونية وردع كل الممارسات التي من شأنها زعزعة الثقة في المعاملات الالكترونية وتخليق مناخ الأعمال، كما تسهر النيابة العامة على تطبيق القانون الجنائي وتطبيق السياسة الجنائية في مجال الجريمة المعلوماتية وذلك من خلال تتبع الجرائم المعلوماتية ومنحها العناية الخاصة وممارسة الدعوى العمومية في حق مقترفيها، فضلا عن تعزيز قدراتها في التصدي لهذه الظاهرة عبر مختلف مراحل الخصومة الجنائية، والاشتغال على الوفاء بالزامات المملكة المغربية في مجال مواجهة للجرائم الإلكترونية.

الكلمات المفتاحية: النيابة العامة، الجريمة المعلوماتية، رئاسة النيابة العامة، الجريمة الإلكترونية، الدليل الرقمي، السياسة الجنائية.

Abstract:

Within the new technological development of information networks, the revolution in communications, computers, smart phones which results a breaking barries. The cyber crime appeared as a new pattern of crime wish had a negative effects on the social, economic and security levels. Which prompted the need to intervene in order to curb this phenomenon.

As the public prosecution considered as part of the judicial authority, wich worker to ensuring the optimum use of digital technology, and also protecting the digital economy by developing monitoring mechanisms to detect cyber crime, and and detering all the practices that would undermine confidence in the electronic transactions. Also, creat a code of ethics in work environment.

The public prosecution ensure the application of criminal law, the application of penal policy to wards cyber crime by tracking computer-related crimes with particular attention. and exercise public proceedings against perpetrators of cyber crimes. As well as, to enhance its ability addressing this phenomenon through all levels of adversarial criminal procedures. Also working on fulfilling the commitments that made by the kingdom of morocco in combating cyber crimes.

Keywords: Public prosecution, presidency of Public prosecution, cyber crime, numerical Guide, penal policy

مقدمة:

عرفت الظاهرة الإجرامية سيما في العقدين الأخيرين تطورا وتناميا غير مسبوق، بالموازاة مع تأثيرات العولمة التي اجتاحت العالم وما صاحبها من تحرير للتجارة العالمية وانفتاح للأسواق وتطور وسائل النقل، هذا إلى جانب الثورة الهائلة الحاصلة في مجال تكنولوجيا المعلوميات والاتصال (العمراني، 2020).

وتعتبر الجرائم المعلوماتية إحدى أهم صور هذه الظاهرة التي عرفت تزايد ملحوظا بالنظر إلى الإقبال على استعمال التكنولوجيا الحديثة وتطور الخدمات المقدمة عبر شبكة الانترنت، خلفت آثار سلبية خطيرة على كافة مناحي الحياة الاجتماعية والاقتصادية والأمنية، وتركت في نفوس الأفراد والمجتمع شعورا بعدم الثقة والاستقرار بخصوص التعامل في الوسائط التكنولوجية.

وكان لهذا التغيير الذي عرفته الجريمة شكلا وموضوعا، تأثيرا موازيا على خطط مكافحتها ومواجهتها التي عرفت بدورها قدرا مماثلا من التطور بشكل يؤدي إلى حصول التناسب المتكافئ بين الخطر الناتج عن الجريمة الإلكترونية ووسائل مواجهتها، مما أصبحت معه المملكة المغربية مضطرة إلى إعادة النظر في أسس ومقومات التخطيط الجنائي والأمني لمكافحة هذه الظاهرة من خلال تبني مجموعة من التدابير والمقاربات الجديدة وملائمة تشريعاتها الجنائية مع هذا النمط الجديد من الجرائم لزجرها والحد من آثارها السلبية (بنسليمان، 2020).

ومن هذا المنطلق تأتي أهمية موضوع دور النيابة العامة في مكافحة الجرائم المعلوماتية على ضوء التشريع المغربي لما يطرحه من إشكالات وتحديات كبير أمام الجهاز القضائي في التصدي للجرائم المعلوماتية، خاصة مع تعقد أساليبها وارتفاع حجمها وتزايد حدتها فترة انتشار جائحة فيروس كورونا المستجد من ناحية، ونظرا لكونه من ناحية ثانية يسلط الضوء على مؤسسة النيابة العامة باعتبارها أداة فعالة في مكافحة الظاهرة الإجرامية المستجدة.

ويهدف الموضوع إلى بيان رصد مظاهر الجريمة المعلوماتية وتطورها في المجتمع المغربي، وكيفية تعامل مؤسسة النيابة العامة في مكافحة هذه الظاهرة والسبل التي تنتهجها للحد من آثارها السلبية وتأمين الاستعمال الأمثل للتكنولوجيا الرقمية، مع الوقوف على أهم الإشكالات والمعيقات التي تحد من نجاعة هذه المواجهة.

والنيابة العامة باعتبارها جزء من السلطة القضائية لا تتوانى عن تفعيل المقتضيات المتعلقة بحماية المجتمع وضحايا الجرائم المعلوماتية، وتسهر على احترام القانون وتطبيقه تطبيقا سليما وتأمين الاستعمال الأمثل للتكنولوجيا الرقمية، وحماية الاقتصاد الرقمي عبر تطوير آليات رصد الجرائم الإلكترونية، وردع كل الممارسات التي من شأنها زعزعة الثقة في المعاملات الرقمية وإرساء مقومات الأمن المعلوماتي داخل المجتمع.

كما تعمل على إعطاء مكافحة الجريمة المعلوماتية العناية التي تستحق وذلك من خلال تتبع الجرائم المعلوماتية ومنحها اهتمام خاصة، وتعزيز قدراتها في التصدي لهذه الظاهرة عبر مختلف مراحل الخصومة الجنائية، فضلا عن تفعيل الوفاء بالزامات المملكة المغربية في مجال مواجهة الجرائم الإلكترونية.

وإذا كان الإلمام بالموضوع من خلال جوانبه الأساسية وتحديد موقعه ضمن التحولات التي يعرفها مجال حماية حقوق الانسان والنظام العام، وتطور التكنولوجيا الرقمية، يستدعيان تحليل الظاهرة المنوه بها في أبعادها القانونية والفقهية وتطبيقاتها العملية، فقد آثرنا التعامل معه من خلال الحاجة إلى طرح الإشكال التالي:

ما مدى مساهمة النيابة العامة في مكافحة الجرائم المعلوماتية لتأمين الاستعمال الأمثل للتكنولوجيا الرقمية وتدعيم الحماية الواجبة للحقوق والحريات بمختلف أبعادها وتعزيز سيادة القانون؟

للإجابة عن هذه الإشكالية ارتأينا أن نتناول هذا الموضوع من خلال محورين، سنخصص المحور الأول للحديث عن دور النيابة العامة في تنزيل مقتضيات القانون الجنائي المعاقبة على الجريمة الإلكتروني وتطبيق السياسة الجنائية في هذا المجال مع الوقوف على أهم الصعوبات المرتبطة بالبحث والتحقيق في الجريمة المعلوماتية. ثم بعد ذلك سنسلط الضوء في المحور الثاني على آليات رصد وتتبع النيابة العامة للجرائم المعلوماتية وسبل تعزيز قدراتها في التصدي لهذا النمط الإجرامي الجديد.

وهكذا ستكون دراستنا للموضوع على الشكل التالي:

أولا: النيابة العامة أداة فعالة لتطبيق القانون وتفعيل السياسة الجنائية في مجال الجرائم المعلوماتية

ثانيا: النيابة العامة بين آليات تتبع الجرائم المعلوماتية وتعزيز قدرات المواجهة

أولا: النيابة العامة أداة فعالة لتطبيق القانون وتفعيل السياسة الجنائية في مجال الجرائم المعلوماتية

بعد تزايد الجريمة وتطور أساليبها بصفة عامة، والجريمة المعلوماتية بصفة خاصة، اهتم المشرع المغربي بتقوية وتفعيل دور النيابة العامة في مكافحة الإجرام وحماية المجتمع، وحاول ما مكن تبسيط المساطر، وأسند لها أدوار مهمة رغبة في إحقاق عدالة سريعة وفعالة ونزيهة تحقق للجميع ما يصبون إليه من شعور بالطمأنينة، وهكذا تسهر النيابة العامة على تفعيل مقتضيات القانون الجنائي المعاقبة على الجريمة الإلكتروني وتطبيق السياسة الجنائية في هذا المجال، مع الحرص على التعامل معها بكل حزم وصرامة –وفقا للقانون- بما في ذلك الأمر بالأبحاث التمهيدية أو المطالبة بإجراء تحقيق وتحريك الدعوى العمومية بشأنها أمام القضاء، وتقديم مطالب وملتمسات واضحة للقضاة بشأن الوقائع الإلكترونية المجرم ترمي إلى تحقيق الردع العام والخاص وحماية الضحايا واستتباب الأمن المعلوماتي.

1.دور النيابة العامة في التحري عن الجرائم المعلوماتية والتثبت من وقوعها ومتابعة مقترفيها

تتولى النيابة العامة تسير الأعمال المتعلقة بالأبحاث التمهيدية وتتلقى الشكايات والوشايات والمحاضر وتتخذ الإجراءات الملائمة بشأنها حفظا للنظام العام والمجتمع، كما تقيم الدعوى العمومية وتمارسها وتطالب بتطبيق القانون وتراقب مدى تطبيقه باعتباره أهم مظاهر مجابهة الجريمة الالكترونية، كما تعمل على تجهيز الملفات الرائجة أمام المحكمة للبت فيها في آجال معقولة، مع السهر على حماية ضحايا الجريمة وتقديم الملتمسات بخصوص الجريمة الإلكترونية المقترفة والتماس عقوبات زجرية تتناسب وخطورتها وخطورة المجرم السيبراني، إلى جانب العمل على تنفيذ

القرارات والأوامر الصادرة عن المحكمة وقضاء التحقيق في القضايا الصادرة في هذا الشأن، وتتولى ممارسة طرق الطعن عند الاقتضاء بخصوص المقررات التي تصدر عن الهيئات القضائية المذكورة.

وإذا كان المشرع قد أوكل للنيابة العامة مهمة التحري عن الجرائم والتثبت من وقوعها والبحث عن المجرمين، فإنه جعل رجال الشرطة القضائية بجميع فئاتهم تحت سلطتها قصد تسخيرهم والاستعانة بهم في أداء مهاما، وهكذا يتلقى وكيل الملك أو الوكيل العام للملك المحاضر والشكايات والوشايات ويتخذون بشأنها ما يرونه ملائما (حلمي و تاشفين، 2005)، ويباشرون بنفسهم أو يأمرون بمباشرة الإجراءات الضرورية للبحث عن مرتكبي الجرائم المعلوماتية.

فهم بذلك يتوفرون على كامل السلطات المخولة للشرطة القضائية أثناء إجراءات البحث، وبمجرد ما يصل إلى علمهم خبر وقوع جريمة من الجرائم المعلوماتية، يمكنهم مباشرة الإجراءات اللازمة لضبط مرتكبها وتقديمه للمحاكمة، ومن حقهم الاستماع إلى أي شخص زهر أن الاستماع إليه سيفيد البحث، وكذا الانتقال إلى عين المكان وإجراء التفتيش والحجز وإلقاء القبض، إلا أنه نظرا لكثرة الأشغال الملقاة على عاتقهم داخل المحكمة وخارجها، تلجأ النيابة العامة إلى إصدار تعليماتها إلى الشرطة القضائية قصد مباشرة الإجراءات الضرورية، وبعد انتهاء المهمة المنوطة به يقوم ضابط الشرطة القضائية بتحرير محضر بذلك يوجهه إلى وكيل الملك مرفقا بجميع الحجج والمستندات (حلمي و تاشفين، 2005، صفحة 26).

وفي إطار المقتضيات القانونية المنظمة للتحقيق الاعدادي، تعمل النيابة العامة على إحالة المحاضر والمشتبه فيهم على قضاة التحقيق بموجب ملتمس بإجراء تحقيق تحدد فيه الجرائم المعلوماتية المطلوب التحري فيها، ثم تسهر على تتبع سير إجراءات التحقيق، وتقدم الملتمسات التي تراها مفيدة للكشف عن الحقيقة.

ومن أجل مواكبة النيابة العامة للتطور الحاصل في ميدان التكنولوجيا والعولمة وما واكبه من أنماط إجرامية مستحدثة، عزز المشرع المغربي دورها بوسائل وآليات جديدة تمكنها من القيام بدورها في حماية المجتمع ومحاربة الجريمة بما فيها الجريمة المعلوماتية وهي:

- ✓ اتخاذ قرار سحب جواز السفر وإغلاق الحدود؛ حيث يحق للنيابة العامة سحب جواز سفر المشتبه فيه الذي ارتكب جريمة من الجريمة المعلوماتية. واقتضت ذلك ضرورة البحث، إما خوفا من فراره أو لخطورة الفعل المرتكب، وذلك لمدة لا تتجاوز شهر واحد، قابلة للتمديد إلى حين انتهاء البحث التمهيدي إذا ثبت أنه هو السبب في عرقلة إتمام البحث.
- ✓ التماس الإذن بالتقاط المكالمات والاتصالات والمراسلات بواسطة وسائل الاتصال المختلفة وتسجيلها، حيث خول المشرع للوكيل العام للملك بعد إجازته من طرف الرئيس الأول لدى محكمة الاستئناف.
- ✓ إصدار أوامر دولية بإلقاء القبض.

وتكمن فعالية الإجراءات المذكورة في تمكين النيابة العامة من الوقت الكافي للتثبت من وقوع الفعل الجرمي الإلكتروني وجمع الأدلة عنه واتخاذ التدابير اللازمة لحماية الضحايا، كما تخول حضور المشتبه فيهم وضمان عدم هروبهم وإفلاتهم من العقاب (حلمي و تاشفين، 2005، صفحة 53 و54).

كما تعمد النيابة العامة إلى حماية أمن الرقمي للأفراد والمجتمع، ليس فقط عبر تفعيل اختصاصاتها الأصيلة المتمثلة في إقامة الدعوى العمومية وممارستها في مواجهة كل شخص اشتبه في ارتكابه أفعال تكون جريمة إلكترونية، وإنما أيضا عبر تتبع الأحكام القضائية الصادرة والطعن فيها كلما اقتضت المصلحة ذلك تكريسا لمبدأ سيادة القانون (رئاسة النيابة العامة، 2020).

2.الصعوبات المرتبطة بالبحث والتحقيق في الجرائم المعلوماتية:

يطرح موضوع البحث والتحقيق في الجرائم المعلوماتية إشكالات مهمة أنتجتها الطبيعة الخاصة والمعقدة لهذا الصنف من الإجرام، وذلك بالنظر إلى خصوصية المجرم المعلوماتي من جهة أولى، ووسائل ارتكاب الجريمة من جهة ثانية؛ فالمجرم المعلوماتي ليس شخصا عاديا بل ينتمي إلى الفئة المتعلمة المحترفة في أغلب الأحيان في ميدان المعلوميات، عارفا بخباياها، له القدرة على التحكم في تصرفاته في علاقته بالآخر، الأمر الذي يطرح صعوبة تعقُب أنشطته غير المشروعة، وبالتالي على أدلة إدانته بارتكاب هذه الجريمة أو تلك، أما من جهة الوسائل، فهي عبارة عن تقنيات متطورة لا يستوعبها إلا المتخصصون، فآليات الجريمة المعلوماتية ليست سيفا أو بندقية أو غيرها، بل لا تحتاج أكثر من مجرم له القدرة على توظيف خبرته في التعامل مع الوسائط التكنولوجية الحديثة لارتكاب الجريمة الرقمية، كالتجسس مثلا والتلاعب بأرصدة البنوك التي لا تحتاج إلا لمسات أزرار، يصعب ضبط نظام عملها من قبل العموم إلا في حدود ضيقة لأنها تقع في بيئة افتراضية لا تترك أي آثار مادية محسوسة خلافا للجرائم التقليدية على اعتبار أن أدلتها ترى بالعين المجردة.

ولعل خصوصية الجريمة المعلوماتية، أبرزت المشكلة الإجرائية للجريمة المعلوماتية خاصة من ناحية كيفية جمع الأدلة الالكترونية ومدى حجتها، وحتى تتوفر في الدليل الالكتروني المشروعية التي تشترطها القوانين في كافة التشريعات (المقداد، 2020).

وبالرجوع إلى قانون المسطرة الجنائية المغربي نجده خاليا من المقتضيات التي تسعف في البحث والتحري فيما يتعلق بالجرائم التي تُقترف في البيئة الإلكترونية، مما يطرح إشكالية شرعية الاستناد إلى القواعد الإجرائية التقليدية في عملية البحث والتحري عن الجرائم المعلوماتية وتتبع مرتكبها، فالقواعد العادية، لا تفي بالغرض المطلوب متى تعلق الأمر بهذا الصنف من الجرائم، والعلة في ذلك أن البحث في الجرائم المعلوماتية يتطلب مهارات وأساليب تقنية وفنية عالية، فضلا عن خصوصية الجريمة وطابعها الافتراض والمعلوماتي، على اعتبار أن هذه الجرائم ذات طبيعة خاصة لتعلقها ببيانات معالجة إلكترونيا وكيانات منطقية غير مادية كما سبقت الإشارة إليه.

وتقتضي إجراءات البحث عن الأدلة وجمعها تأسيسا على مبدأ الشرعية الإجرائية أن تكون موافقة ومحددة وفق القانون ولا تخرج عن روح نصوصه، وبالتالي فإن التوسع في مباشرة إجراءات أو في تفسير الإجراءات المقررة فإنه يهدد حقوق وحريات الأفراد، لذلك فإن النصوص الخاصة ببعض الإجراءات بمفهومها التقليدي لا ينبغي إعمالها بشأن الجريمة المعلوماتية مباشرة، باعتبار أن هذه النصوص تمثل قيدا على الحرية الفردية، ومن ثم يصبح القياس على الأشياء المادية محظورا لمنافاته الشرعية الإجرائية (مقوش، 2018).

ومن أجل ذلك وفي إطار تعزيز آليات مكافحة الجريمة المعلوماتية، صادق المغرب سنة 2018 على اتفاقية بودابست المتعلقة بالجريمة المعلوماتية الشي الذي وضع المملكة المغربية في مصاف البلدان الرائدة في مجال التشريعات المتقدمة ومنحها آلية متطورة لمكافحة الجرائم المرتكبة بواسطة أنظمة المعلوميات.

وقد أقرت اتفاقية بودابست مجموعة من القواعد الإجرائية التي تهم التحقيق وجمع الأدلة والتعاون القضائي في مكافحة الإجرام المعلوماتي، كالمواد 16 إلى 21 منها البحث والتحري عن مرتكبي هذه الجرائم، التي يتضح من خلال مطابقتها مع القواعد الإجرائية الواردة في قانون المسطرة الجنائية والمقررة لكافة الجرائم أن هذه الأخيرة تتسع لتشمل في تطبيقها الجريمة الإلكترونية مع ضرورة إدخال بعض التعديلات على المسطرة الجنائية.

وبالرجوع إلى أحكام قانون المسطرة الجنائية المغربي نجده قد ألزم في المادة 57 ضابط الشرطة القضائية، الانتقال في الحال إلى مكان ارتكاب الجريمة وإجراء المعاينات المفيدة والحفاظ على الأدلة القابلة للاندثار، وعلى كل ما مكن أن يساعد على إظهار الحقيقة وحجز الأدوات التي استعملت في ارتكاب الجريمة أو التي كانت معدة لارتكابها، وكذا جميع ما قد يكون ناتجا عن هذه الجريمة بغض النظر عن طبيعة هذه الأخيرة، مع إلزام كل شخص ساهم في الإجراءات أثناء البحث أو التحقيق بالحفاظ على السرية تحت طائلة العقوبات المقررة في مجموعة القانون الجنائي.

كما نصت المادتين 59 و60 من قانون المسطرة الجنائية المغربي على مقتضيات عامة تنظم التفتيش كإجراء تخضع له كافة الجرائم بغض النظر عن طبيعتها بما فيها الجريمة الإلكترونية، في حين منحت المادة 60 من نفي القانون لسلطات البحث والتحري صلاحية حجز الأوراق والوثائق أو أشياء أخرى في حوزة الأشخاص أو المستندات والأشياء المتعلقة بالأفعال الإجرامية، رغم أن بعض التشريعات المقارنة ذهبت صراحة إلى التنصيص على حجز البيانات المخزنة في أنظمة الكمبيوتر كالتشريع الفرنسي والبلجيكي (مقوش، 2018، صفحة 195).

ويعتمد في إجراء المعاينة الإلكترونية بحثا عن الأدلة الرقمية على فحص مجموعة من مصادر الدليل في البيئة الرقمية التي ارتكبت فيها الجريمة المعلوماتية، والمتمثلة عادة في مكونات أجهزة الحواسيب الخاصة بالجاني والمجني عليه وملحقاتها وكذا أنظمة الاتصال بالأنترنت.

وحتى تقوم النيابة العامة بالمهام المنوطة بها وخصوصا فيما يتعلق بالكشف والتصدي للجرائم المعلوماتية، كونها تعودت على التحقيق في الجرائم التقليدية دون هذا النوع من الجرائم، يجب أن تتوفر على مجموعة من المهارات والمقومات، وتكون على دراية كبيرة بجهاز الحاسوب الآلي وكل ما يرتبط به وعموما بكل المسائل المعلوماتية، مع التكوين المستمر تبعا للتطورات التي يعرفها هذا المجال والذي يتطور بسرعة فائقة (المقداد، 2020، صفحة 195).

لذلك مهما تطورت الترسانة القانونية الإجرائية لاستيعاب طرق وآليات التحقيق في مثل هذه الجرائم، فإنها ستظل قاصرة عن تحقيق المبتغى ما لم تكون هناك كوادر مؤهلة تأهيلا قانونيا ومعلوماتيا مستمرا، يواكب كل المستجدات التي تعرفها التقنيات الحديثة التي لا تعرف معنى التوقف، والتي يكون بإمكانها التحقيق والكشف عن هذه الجرائم التي تقع في بيئة افتراضية لا مادية.

وتعتبر الأدلة الجنائية الوسيلة التي تعتمد عليها النيابة العامة في إثبات الاتهام وتقصي الحقائق حول الوقائع والأشخاص والأشياء وصولا إلى العدل كغاية يتطلع إليها كل فرد في المجتمع، وإذا كانت ضرورة الإثبات مرتبطة بكل الجرائم بمختلف أشكالها وأنواعها، بالنسبة للجرائم المعلوماتية يحمل في طياته الكثير من الخصوصية والصعوبة، فانفصال مفهوم الجريمة كبناء قانوني عن الوسيلة التي ترتكب بها يختلف في هذا السياق العديد من الإشكالات المرتبطة بالإثبات في المجال الجنائي، فالجريمة المعلوماتية لا تترك أثرا خارجيا يسهل معه إثباتها إذ يتم نقل المعلومات بالنبضات الإلكترونية، وأن الجاني يستطيع تدمير دليل الإدانة في أقل من ثانية، كما أنها تحتاج إلى خبرة فنية وتقنية يصعب على المحقق التقليدي التعامل معها، إضافة على أنها تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبها ناهيك على أنها تحتاج إلى قمة الذكاء والمهارة في ارتكابها (العلوي، 2004).

فإثبات الجرائم المعلوماتية يحتاج إلى طرق تقنية تتناسب مع طبيعتها، بحيث يمكنها فك رموزها وترجمة نبضاتها وذبذباتها إلى كلمات وبيانات محسوسة ومقروءة تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنية والعلمية الخاصة (بنسليمان، 2020، صفحة 139).

والدليل الرقمي لا يشمل فقط ذلك المستخرج من الحاسوب الآلي وإنما جميع الأجهزة الالكترونية والمعلوماتية الأخرى وشبكات الاتصالات كيفما كان نوعها، ويعتبر هذا الدليل من بين وسائل الإثبات المقبولة والتي يمكن اعتمادها لإثبات جريمة من الجرائم المعلوماتية، شريطة اقتناع القاضي بها طبعا والذي يتمتع في هذا الإطار بسلطة واسعة في تقدير الأدلة، والقضاء المغربي بطبيعة الحال يأخذ بالدليل الإلكتروني ويعتمد عليه في الإثبات (المقداد، 2020، صفحة 447).

ثانيا: النيابة العامة بين آليات تتبع الجرائم المعلوماتية وتعزيز قدرات المواجهة

أمام انتظارات مجتمع يعيش لحظات تحول وتطور متسارع في المجال الرقمي وفي العلاقات بين أفراده ومؤسساته بالمجال التكنولوجي، وأمام مجتمع يتطلع إلى تكريس قضاة فعال في خدمة الاقتصاد الرقمي والمواطن وسيادة القانون في الفضاء الرقمي وتأمين الاستعمال الأمثل للتكنولوجيا المعلوماتية، تسهر رئاسة النيابة العامة على تتبع كل القضايا المتعلقة بالجرائم المعلوماتية مع النيابات العامة بمختلف محاكم المملكة، وتعمل على فتح قناة التعاون القضائي بين الدول لمكافحة هذا النمط الإجرامي الجديد، كما تقوم بتنفيذ الالتزامات الملقاة على عاتق ببلادنا بمقتضى اتفاقية بودابست للجرائم المعلوماتية، بالإضافة إلى حرصها على تنزيل مضامين السياسة الجنائية الوطنية في مجال مكافحة الجريمة المعلوماتية من خلال رصد الظاهرة الاجرامية وتعزيز قدرات قضاتها في مستجدات الإجرام السيبراني، ورصد تحولات الجريمة المعلوماتية عبر تتبع تحولاتها وإجراء إحصاءات حول الأبحاث والمتابعات والقرارات القائمة والصادرة بشأنها.

1.تتبع الجريمة وإيلاء عناية خاصة بتفاقم الجريمة الالكترونية:

يعد تتبع الجريمة وإيلاء عناية خاصة للظواهر الإجرامية المستفحلة أو الجديدة من أهم أوجه مكافحة الجريمة، فعن طريقه تستطيع تحديد مدى استفحال الظاهرة وانتشارها وبالتي تحديد أوجه تدخلها للقضاء عليها وسبل

احتوائها، وفي هذا الإطار تعمل رئاسة النيابة العامة على تتبع الجرائم المعلوماتية ورصد حركيتها وتحولاتها ومظاهرها وتطور أشكالها الجديدة.

وعلى ضوء ذلك، عرفت السنوات الأخيرة خاصة مع بداية ظهور فيروس كورونا المستجد انتقالا كبير في نطاق الظاهرة الإجرامية من العالم الواقعي إلى العالم الافتراضي الذي سجلت فيه الجريمة المعلوماتية أعلى مستوياتها، فبمجرد الإعلان عن انتشاره عالميا، تزايدت عمليات النصب والاحتيال المعلوماتي وتسارعت وثيرة عمليات البيع غير المشروعة عبر الإنترنت، فضلا عن استفحال ظاهرة الابتزاز والتخويف والترهيب الإلكتروني عبر نشر الإشاعات والأكاذيب عن تفشي فيروس كورونا وانتشاره (حسان، 2020).

كما رصدت النيابة العامة أن بعض الظواهر التي تمثل الجانب السلبي للتكنولوجيا طفت على السطح ومن بينها الابتزاز الجنسي عبر الأنترنت، الذي يبقى إحدى الظواهر الإجرامية الخطيرة التي انتشرت بشكل ملفت في الآونة الأخيرة بالنظر إلى تصاعد نسبة هذه الجرائم وما تخلفه من أضرار بليغة تلحق الضحايا وأسرهم، إذ أبانت حالات هذه الجريمة أن الضحية يتعرض لأضرار نفسية بليغة. فضلا عن الأضرار ذات الطابع الاجتماعي التي قد تؤدي في كثير من الأحيان إلى تدمير العلاقات الزوجية والعلاقات الأسرية عموما.

وقد أكدت النيابة انتشار بعض التقنيات في مجال تشفير المواقع الإلكترونية وقواعد البيانات، والذي يجسد تقنية تسمح للمجرمين بالولوج إلى المواقع الإلكترونية وقواعد البيانات وتشفيرها مع ابتزاز الضحايا، كما تم التصدي لحالات قرصنة المعلومات الخاصة بالبطائق الإلكترونية المعروفة بـ"Skiming" والتي تستعمل لقرصنة الأرقام السرية لبطائق بنكية، مما يمكن من الاحتيال وسرقة أموال أصحابها. (عبد النباوي، 2021)

وقد أكد تقرير رئاسة النيابة العامة المتعلق بتنفيذ السياسة الجنائية لسنة 2020، أن الجريمة المعلوماتية عرفت تزايدا مهما بالنظر إلى الاقبال الملحوظ على استعمال التكنولوجيا الحديثة وتطور الخدمات المقدمة على شبكة الانترنت، وأكدا من جهة ثانية أن النيابة العامة بالمغرب تابعت 239 شخصا بسبب ارتكابهم لجرائم المس بنظم المعالجة الآلية للمعطيات فتحت في مواجهتهم 117 قضية.

كما أضحت بعض الجرائم التقليدية ترتكب باستعمال الوسائل المعلوماتية والتي وصلت عدد القضايا فيها إلى 438 شخصا وتبع من خلالها 498 متهما، وشكل منها جريمة النصب عن طريق الانترنت ما يقدر 66 قضية توبع خلالها ما مجموعه 74 متهما، وجاءت جريمة التحرش الجنسي عن طريق الوسائط الإلكترونية ب 108 قضية، بينما جريمة الابتزاز الجنسي ما يعادل 226 قضية توبع خلالها261 شخص بنسبة تجاوزت 5 في المئة من مجموع القضايا المسجلة في هذا النمط من الجرائم (رئاسة النيابة العامة، 2020، صفحة 333وما بعدها).

وفي نفس السياق، سجلت قرابة 24 قضية توبع خلالها 35 شخصا بخصوص الجرائم ذات الصلة بالمحتوى المرتكبة باستعمال الوسائل المعلوماتية وفقا لاتفاقية بودابست، كاستغلال القاصرين في مواد إباحية، وهو الأمر الذي يمكن أن يعزى إلى عدم قابلية هذا النوع من الجرائم إلى البروز، إذ نادرا ما تصل هذه القضايا إلى علم أجهزة العدالة، بالنظر إلى كون الجناة يظلون في منأى عن أعين الشرطة القضائية بسبب استغلالهم لما يتيحه الويب المظلم "Dark Web" من إمكانية لإخفاء هوياتهم.

وباستقراء التقرير السابق يتضح بأن جريمة القيام بطريقة غير مشروعة وبأي وسيلة كانت بقصد الاستغلال التجاري بخرق متعمد لحقوق المؤلفين والحقوق المجاورة تأتي في مقدمة الجرائم المعلوماتية المتعلقة بانتهاك حقوق المؤلف والحقوق المجاورة، حيث تم تسجيل 16 قضية توبع من خلالها 16 شخصا، في مقابل قضيتين تم تسجلهما بخصوص جريمة التقليد الالكتروني.

2. بحث سبل التعاون القضائي الدولي وتعزيز قدرات مواجهة الجرائم المعلوماتية:

أمام تزايد الجريمة المعلوماتية وازدياد حدتها عبر الحدود الوطنية والدولية، أصبح من الصعب على أي دولة مهما بلغت قوتها مكافحتها بمفردها، الأمر الذي دفع إلى تعزيز سبل التعاون الدول فيما ينها من أجل التصدي لهذا النمط الإجرامي الجديد وإرساء مقومات الأمن المعلوماتي (أمين و عبدالسلام، 2016).

وفي هذا الإطار، ومن أجل مكافحة الجرائم المعلوماتية وحرصا على اتخاذ كافة الوسائل التي تحول دون إفلات المجرم السيبراني من العقاب، تقُوم النيابة العامة بدور مهم في إطار مسطرة تسليم المجرمين، ولاسيما في الوقت الحاضر الذي أصبح فيه من السهل على المجرمين الفرار والانتقال من دولة إلى أخرى في أقصر وقت وبأقل جهد، كما تضطلع النيابة العامة بدور أساسي في تدبير الإنابات القضائية الوطنية والدولية في الإجرام المعلوماتي، حيث تقوم من بالتوصل بالإنابات القضائية الصادر عن النيابة العامة من مختلف محاكم المملكة أو الصادرة عن محاكم أجنبية من أجل بحث بعض الأفعال الإلكترونية محل التحقيق والبحث. كما أحالت السلطات القضائية المغربية خلال سنة 2020 على رئاسة النيابة العامة إنابة قضائية دولية قصد توجيهها للتنفيذ إلى سلطات قضائية بدول أخرى ثلاثة قضايا متعلقة بالجريمة المعلوماتية، وقد التمست الحصول على نسخ من محاضر ووثائق أو معلومات بحوزة السلطات القضائية الأجنبية، وذلك من أجل لاستكمال أبحاثها المفتوحة لديها بخصوص جرم معلوماتي معين (رئاسة النيابة العامة، 2020، صفحة 162).

ولما كان تأهيل الشرطة القضائية والنيابة العامة وقضاة الحكم والتحقيق بشكل يسمح بتكوين أجهزة قضائية متخصصة قادرة على التعامل مع الجريمة المعلوماتي، وعلى طرق وكيفية استخدام أجهزة المعلومات، وطرق البحث والتحقيق وجمع الأدلة فيها من أهم مداخل مواجهة الجريمة المعلوماتية.

عملت رئاسة النيابة العامة على اعطاء أهمية خاصة لتعزيز قدرات النيابة العامة للتصدي لهذه الجرائم. إذ بالنظر إلى خصوصية وأهمية البحث في الجرائم المعلوماتية، وإلى صعوبة جمع الأدلة الرقمية المرتبطة بها، فقد حرصت رئاسة النيابة العامة على مشاركة قضاة النيابة العامة الذين تم تعيينهم كنقط ارتكاز، في ندوات ودورات تكوينية بالمغرب عن الجرائم المعلوماتية والدليل الرقمي بالتعاون مع شركاء دوليين، وتوعيتهم بالأساليب المتطورة والمستجدة في المجال الإلكتروني.

كما استفاد المغرب من التجربة الدولية في المجال الإلكتروني، حيث أنه تحصل على مجموعة من برامج المساعدة التقنية، خاصة في إطار برامج Cyber Sud و Glacy التي تنفذ بدعم ورعاية مجلس أوروبا حيث كان من

نتائجها تكوين متخصصين في الجريمة المعلوماتية في صفوف القضاة وضباط الشرطة القضائية وإدراج الجرائم المعلوماتية ضمن برامج التكوين الأساسي للقضاة وكذلك بالمعهد الملكي للشرطة. (اللبار، 2020)

وعلى صعيد آخر، تشتغل رئاسة النيابة العامة على الوفاء بالتزامات المملكة المغربية في مجال التصدي للإجرام المعلوماتي، فبعد المصادقة على اتفاقية بودابست للجرائم المعلوماتية ودخولها حيز النفاذ ابتداء من فاتح أكتوبر 2018، توصلت المملكة المغربية بطلبات ترمي إلى حفظ بيانات الكمبيوتر المخزنة في إطار شبكة 7/24 المحدثة من قبل الاتفاقية المذكورة، وتم التنسيق مع النيابات العامة المختصة لاتخاذ الإجراءات اللازمة قصد ضمان تنفيذها. كما تم إحداث شبكة من قضاة النيابة العامة للوفاء بالتزامات المملكة الدولية، في إطار شبكة 24/7 التي تقضي اعتماد ديمومة وطنية على مدار اليوم طيلة أيام السنة (24 ساعة/ 24 ساعة وسبعة أيام في الأسبوع)، للقيام بمهام التعاون القضائي الدولي وفاء بالتزامات المملكة المترتبة عن المصادقة على الاتفاقية المذكورة (عبد النباوي، 2021).

خاتمة:

تُبرِز الإحصائيات الخاصة بالجرائم المعلوماتية حسب تقرير رئاسة النيابة العامة حول تنفيذ السياسة الجنائية، مدى حجم المسؤوليات الكبرى الملقاة على مؤسسة النيابة العامة في حماية المجتمع وحفظ الأمن المعلوماتي للأفراد والمؤسسات، نظرا إلى تفاقم المعطيات المتعلقة بالإجرام المعلوماتي.

وإذا كانت السياسة الجنائية المغربية تركز على محاربة الجرائم التقليدية المرتكبة ضد الأشخاص أو ضد الأخلاق والنظام العام باعتبارها تشكل تهديدا حقيقيا لقيم المجتمع واستقراره، فإن الظرفية فرضت على النيابة العامة الاهتمام بحماية المجال والفضاء الإلكتروني حفظا للأمن المعلوماتي وتأمين الاستعمال الآمن للتكنولوجيا الرقمية وحماية الاقتصاد الرقمي.

وذلك عبر رصد واقع الإجرام الإلكتروني وتتبع مساراته وتحولاته قصد التدخل الفوري للحد من خطرته وحفظ النظام العام وإرساء سيادة القانون، مع اتخاد آليات وتدابير موازية تهدف إلى الانخراط الإيجابي للنيابة العامة في بناء استراتيجيات وخطط وطنية لمكافحة هذه الظاهرة، وكذا تعزز قدرات قضاتها في البحث والتحري عن الجرائم المعلوماتية واستيعاب ابعادها وعناصرها المعقدة، مع فتح آليات التعاون والتواصل الدولي في التصدي ومحاصرة هذه الجرائم.

وتتعزز هذه المحاصرة أيضا من خلال دورها التقليدي في مكافحة الجريمة حيث تتولى النيابة العامة تسير الأعمال المتعلقة بالأبحاث التمهيدية في الجرائم المعلوماتية وتتلقى الشكايات والوشايات وتتخذ الإجراءات الملائمة بشأنها حفظا للأمن الرقمي للأفراد والمجتمع، كما تقوم بمقاضاة ومتابعة مرتكبي هذه الجرائم قصد تحقيق العدالة في حقهم، فضلا عن أنها تُقدم باسم القانون جميع المطالب والملتمسات الرامية إلى حماية الضحايا الجرائم الإلكترونية والتماس عقوبات زجرية تتناسب وخطورة الأفعال المرتكبة، وتتولى ممارسة طرق الطعن عند الاقتضاء بخصوص المقررات التي تصدر عن المحكمة والتي لا ترها تحقق الحماية المنشودة لأمن واستقرار المجتمع.

وننتهي في هذه الدراسة إلى الخروج بالتوصيات التالية:

- ✓ توفير الإمكانات المالية والبشرية التي تمكن النيابة العامة من حسن قيام بمهامها، وذلك من خلال الرفع من الموارد التقنية واللوجستيكية التي تهم تمكين النيابة العامة من آليات بحث الجرائم المعلومية وتتبع مرتكبيها، مع ضرورة تأهيل قضاة النيابة العامة ورفع عددهم وعدد الموظفين الساهرين على تدبير القضايا في جناح النيابة العامة بمختلف المحاكم.
- ✓ من أجل ضمان فعالية أكثر للقوانين المؤطرة للجرائم المعلوماتية وتحقيقها للحماية المطلوبة، كان لزاما على المشرع العمل على التحيين المستمر لترسانته التشريعية نظرا لما يعرفه الإجرام اسيبراني من تطور مستمر يوما بعد يوم من جهة، ومن أجل تمكين النيابة العام من التكييف القانوني لوقائع المحال علها بما يتناسب مع خطورة الأفعال المقترفة وضرورة الانضباط لمبدأ الشرعية الجنائية في اتهامها من جهة ثانية.
- ✓ العمل على نشر الوعي في صفوف المواطنين بمخاطر الجريمة الإلكترونية وضرورة اتخاذهم الحيطة والحذر في استعمال وسائل التواصل الإلكتروني والشبكة العنكبوتية من أجل تقليص عدد ضحايا الإجرام المعلوماتي.
- ✓ ندعو إلى إحداث مراكز وجهات خاصة بمراقبة الجرائم المعلوماتية تتولى رصد حجمها وتتبع مساراتها وتحولاتها الممكنة، مع وضع استراتيجية متكاملة، تشمل إلى جانب أدوار النيابة العامة كافة الفعالين والمتدخلين في العملية التشريعية والأمنية من أجل مكافحة ناجعة للجرائم المعلوماتية.

قائمة المراجع:

1) أعزان، أمين، و جاكيي، عبدالسلام. (2016). الحماية الجنائية للمعطيات في المجال المعلوماتية. المجلة المغربية للقانون الجنائي والعلوم الجنائية، العددالثالث.

2) البلغيتي، عبد الله العلوي. (2004). الإجرام المعاصر وأساليب مواجهته، السياسة الجنائية بالمغرب: واقع وأفاق. منشورات جمعية نشر المعلومة القانونية والقضائية، سلسلة الندوات والأيام الدراسية العدد 3.

3) الحافظي، نجاة، (2017)، الشرح الوجيز لقانون المسطرة الجنائية، الطبعة الأولى، الأحمدي، الدار البيضاء.

4) اللبار، أيوب، (2021 يونيو 19)، السياسة الجنائية في مواجهة جرائم المس بنظم المعالجة الالية للمعطيات . Récupéré sur https://www.droitetentreprise.com/20237/

5) بنسليمان، عبد السلام. (2020). الإجرام المعلوماتي في التشريع المغربي دراسة مقارنة في ضوء آراء الفقه وأحكام القضاء، الطبعة الثالة، دار الأمان، الرباط.

6) بيشا، حسان. (2020). الظاهرة الإجرامية وتحولاتها زمن جائحة كورونا. مجلة الدراسات المندمجة في العلوم الاقتصادية والقانونية والتقنية والتواصل، صفحة 4.

7) رئاسة النيابة العامة. (2020). تقرير رئيس النيابة العامة حول تنفيذ السياسة الجنائية وسير النيابة العامة.

8) سعيد مقوش. (2018). الجريمة المعلوماتية وأزمة الشرعية الإجرائية. السياسة الجنائية بالمغرب الواقع والآفاق، مطبعة الأمنية، الرباط.

9) سليمان المقداد. (2020). محاربة الجرائم المعلوماتية في القانون الجنائي المغربي. المجلة الدولية للأبحاث الجنائية والحاكمة الأمنية، العدد الثالث.

10) محمد عبد النباوي. (17 مارس، 2021). كلمة الوكيل الوكيل العام للملك لدى محكمة النقض، رئيس النيابة العامة في افتتاح أشغال ندوة حول حقوق الإنسان والتحدي الرقمي. تم الاسترداد من https://www.pmp.ma

11) مصطفى حلمي، و رشيد تاشفين. (2005). مرشد قاضي النيابة العامة، الطبعة الأولى. الشركة الجديدة للطباعة والنشر، الدار البيضاء.

12) نور الدين العمراني. (2020). القانون الجنائي المغربي وتحديات الإجرا المنظم العابر للحدود أية مواكبة؟ المجلة الدولية للأبحاث الجنائية والحكامة الأمنية، العدد الثالث.

الجريمة الالكترونية بين دوافع ارتكابها واليات مواجهتها: الإستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم الالكترونية أنموذجا

Cyber crime between the motives for its commission and the mechanisms to confront it - the security strategy of the Algerian state in combating cybercrime as a model

د.ايمان بومدين/ جامعة المدية/ الجزائر

Dr. Iman Boumediene/ Medea University/ Algeria

د.حنان بن مزيان/ جامعة المدية/ الجزائر

Dr. Hanan bin Meziane/ Medea University/ Algeria

ملخص الدراسة:

في السنوات الاخيرة شهد العالم عدة تغيرات وتطورات بما فيها التطور الذي شمل مجال التقنية ، مما نتج عنه استعمال الحاسب الالي وشبكة الانترنت في جميع الميادين بحيث يعد هذان الاختراعان من اهم الاختراعات في تاريخ البشرية ، لكن وبالمقابل نجد انه تم استغلال هذه الوسائل بطرق غير مشروعة ، الامر الذي انجر عنه ارتكاب جرائم عدة من بينها ما يسمى الجريمة الالكترونية كنشر الفيروسات التي تؤدي الى تدمير اجهزة الحاسوب والمعلومات وكذا القرصنة الالكترونية والدخول غير المشروع الى الفضاء الالكتروني للغير ، بحيث اصبح هذا النوع من الجرائم من اخطر الظواهر الاجرامية المستحدثة في المجتمع الجزائري ، وساهم بدوره في ظهور مجرمين ذوي خصائص مختلفة عن المجرمين التقليديين.

الكلمات المفتاحية: الجريمة، الجريمة الالكترونية، الأسباب

Abstract:

In recent years, the world has witnessed various changes and developments , including the development of the field of technology, leading to the use of computers and the internet in all fields . Thus , these two inventions are invention are among the most significant inventions in the history of humankind. Otherwise , we find that these means have been exploited illegally , resulting in the commission of several crimes , among the; there is the so-called cybercrime , such as spreading viruses which cause the destruction of computers and information , as well as electronic piracy and illegal entry into cyberspace of others , therefore , this type of crime has become one of the most serious criminal phenomena introduced in the Algerian society .as it contributed to the emergence of criminals with different characteristics from the traditional ones.

Keywords: crime, cybercrime, causes.

مقدمة:

لازمت الظاهرة الإجرامية المجتمعات البشرية منذ أقدم العصور وتطورت بتطورها ، وبما ان الانسان دائما في تطور مستمر بفضل ثورة المعلومات والتكنولوجيا المتطورة فإننا نجد العلماء والمختصين وأفراد المجتمع يحاولون الاستفادة منها ، وبالمقابل نجد المجرمين يحاولون كذلك الاستفادة من هذا التقدم التقني، بحيث اصبحت التكنولوجيا

متاحة لكل الفئات المجتمعية، بحيث استطاع المجرمين اكتساب خبرات ومهارات اكثر في تعاملهم مع الانترنت وارتكابهم للجرائم الالكترونية عبر الاقمار الصناعية، فلم تعد جرائمهم تقتصر على اقليم دولة واحدة بل تجاوزت كل الحدود الاقليمية، وهي جرائم مستحدثة تمثل ضربا من ضروب الذكاء الاجرامي، ولهذا كان من الصعب ادراجها ضمن الاوصاف الاجرامية والجنائية التقليدية في القوانين الجنائية الوطنية والدولية لما لها من اساليب حديثة ومتعددة، لذا وجب على المشرع القانوني تطوير الانظمة والقوانين الجنائية بذكاء مماثل للذكاء الاجرامي وبدقة وحكمة متناهية ومحاولة تكييفها حسب هذا النوع من الجرائم، ومن خلال ما سبق يمكن الوصول الى سبل مواجهة هذه الجرائم الالكترونية من خلال تعاون الانظمة الدولية وفهمها للسبل الشرعية والعمل بها في مكافحة هذا النوع من الجرائم المستحدثة ، وبهذا يقل خطرها ويسعد أفراد المجتمع ويعيشون في امن وسلام. ومن خلال ما سبق يمكن طرح التساؤل التالي: اين تكمن الدوافع الحقيقية في ظهور مثل هذا النوع من الجرائم؟ وماهي آليات ووسائل مواجهتها؟

أهمية الدراسة:

تكتسي دراستنا هذه أهميتها من نوعية الموضوع المعالج، إلى جانب المقاربة المعتمدة في سياقه، حيث تهدف الدراسة الحالية إلى التعريف بظاهرة جديدة هي الجريمة الالكترونية التي بدأت في الظهور والانتشار وارتبطت بتكنولوجيا الحاسبات الآلية ، مما أسفر عن تميزها بمجموعة من الخصائص تختلف عن غيرها من الجرائم مما يستتبع ضرورة التعامل معها بما يتلاءم من هذه الخصوصية وكيفية مواجهتها سواء من الناحية التقنية وهو عمل المتخصصين في مجال تكنولوجيا المعلومات أو من الناحية القانونية والأمنية وهي مهمة المشتغلين بالقانون والآمن بالإضافة الى استفادة الباحثين والقضاة ورجال الأمن من توصياتها والبناء عليها وتطويرها لإجراء دراسات معمقة في مجال تقنية المعلومات.

أهداف الدراسة:

تتمثل اهداف هذه الدراسة فيما يلي:

1. محاولة تحديد ماهية الجريمة الالكترونية والمشكلات الموضوعية والإجرائية التي تثيرها،
2. محاولة الوصول لفهم ظاهرة الجريمة الالكترونية والتهديدات الناجمة عنها وعن مدى درجة خطورتها.
3. محاولة التعمق في كيفية تحديد أهم آليات ووسائل مواجهة الجريمة الالكترونية من خلال عرض الإستراتيجية الأمنية للدولة الجزائرية في مكافحة الجرائم الالكترونية أنموذجا.

1. التحديد المفاهيمي للجريمة الالكترونية:

لا يوجد اجماع على تعريف الجريمة الالكترونية من حيث كيف تعرف او ما هي الجرائم التي تتضمنها الجريمة الالكترونية، وكما يقول **فان هلست وونيف** هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل من الجريمة، في اغلب الاحيان تستخدم مصطلحات الافتراضية والحاسوب والالكترونية والرقمية.

ويتراوح تعريف الجريمة الالكترونية بين الجرائم التي ترتكب بواسطة الحاسوب الى الجرائم التي ترتكب بآي نوع من المعدات الرقمية، وتعريف الجرائم الالكترونية باختصار على انها الجرائم التي ترتكب باستخدام الحاسوب والشبكات والمعدات التقنية مثل الجوال أو الهاتف النقال.) التنظيم القانوني والجرائم الالكترونية :مابين امن المعلومات وتقييد الحريات(2018 ,

عرفت بأنها الممارسات التي توقع ضد فرد او مجموعة مع توفر باعث إجرامي، بهدف التسبب بالأذى لسمعة الضحية عمدا، او الحاق الضرر النفسي والبدني به سواء اكان ذلك بأسلوب مباشر او غير مباشر، بالاستعانة بشبكات الاتصال الحديثة كالانترنت وما تتبعها من ادوات كالبريد الالكتروني وغرف المحادثة، والهواتف المحمولة.

أدت الحداثة التي تتميز بها الجريمة الالكترونية واختلاف النظم القانونية والثقافية بين الدول إلى اختلاف في مفهوم الجريمة الالكترونية من بينها:

حسب اللجنة الاوروبية فان مصطلح الجريمة الالكترونية يضم كل المظاهر التقليدية للجريمة مثل الغش وتزييف المعلومات ونشر مواد الكترونية ذات محتوى مخل بالأخلاق او دعوى لفتن طائفية.

حسب منظمة التعاون الاقتصادي للجريمة المرتكبة عبر الانترنت: هي كل سلوك غير مشروع أو غير اخلاقي أو غير مصرح به يتعلق بمعالجة الية للبيانات ونقلها) .التنظيم القانوني والجرائم الالكترونية :مابين امن المعلومات وتقييد الحريات(2018 ,.

وعليه يمكن القول ان الجريمة الالكترونية تتمثل في ممارسة كل الجرائم التقليدية ولكن بطريقة مستحدثة اي باستخدام القطاع المعلوماتي والتطور التكنولوجي.

2. خصائص الجريمة الالكترونية:

من المتبادر الى الذهن عند الحديث عن خصائص الجريمة الالكترونية ان الجاني له دور كبير في معظم حالاتها و نبني عليها تصور العمدية من الجاني، لأنه في الغالب يتعمد التدخل في مجالات النظام المعلوماتي المختلفة مثل مجال المعالجة الالكترونية للبيانات،ومجال المعالجة الالكترونية للنصوص، والكلمات الالكترونية، ففي مجال المعالجة الالكترونية للبيانات يتعمد الجاني ادخال البيانات التي يمكن ان تساعده في الحصول على المعلومات التي من خلالها تتم الجريمة الالكترونية بواسطة الحاسب الآلي، وفي مجال المعالجة الالكترونية للنصوص والكلمات يتمكن مستخدم الحاسب الالي كتابة الوثائق المطلوبة بدقة متناهية بفضل الادوات الموجودة تحت يده ، وإمكانيات الحاسب الالي ايضا لها دور كبير في تيسير ارتكاب الجريمة، فكلما ارتفعت إمكانيات الحاسب تمكن المستخدم من التصحيح ، والتعديل والمحو ، والتخزين ، والاسترجاع ، والطباعةوغيرها (العريان، 2004، صفحة 37)

وبعد هذا العرض لبعض الصور من الجريمة الالكترونية يتضح ان خصائصها يمكن بيانها على النحو التالي:

- ✓ مرتكب الجريمة الالكترونية في الغالب شخص يتميز بالذكاء، والدهاء ذو مهارات تقنية عالية ودراية بالأسلوب المستخدم في مجال انظمة الحاسب وكيفية تشغيله، وكيفية تخزين المعلومات والحصول عليها، في حين ان مرتكب الجريمة التقليدية في الغالب شخص امي بسيط متوسط التعليم.
- ✓ مرتكب الجريمة الالكترونية قد يكون منسجما اجتماعيا قادرا ماديا، لأن باعثه على ارتكاب جريمته في كثير من الأحيان رغبته في قهر النظام، وهذه الرغبة قد تزيد عنده على رغبته في الحصول على المال، في حين أن مرتكب الجريمة التقليدية في الغالب يكون غير منسجم اجتماعيا ورغبته في الحصول على المال تفوق بكثير اي رغبة اخرى.
- ✓ تقع الجريمة الالكترونية في مجال المعالجة الالية للمعلومات، وتستهدف المعنويات لا الماديات وهي بالتالي اقل عنفا وأكثر صعوبة في الاثبات، لأن الجاني مرتكب هذه الجريمة لا يترك وراءه أي أثر مادي خارجي ملموس يمكن فحصه، وهذا يعرقل اجراءات اكتشاف الجريمة ومعرفة مرتكبها، بخلاف الجريمة التقليدية التي عادة ما تترك وراءها دليلا

ماديا او شهادة شهود أو غيرها من ادلة الاثبات، كما ان موضوع التفتيش والضبط قد يتطلب احيانا امتداده الى اشخاص آخرين غير المشتبه فيه او المتهم.

- ✓ الجريمة الالكترونية ذات بعد دولي، اي انها عابرة الحدود، فهي قد تتجاوز الحدود الجغرافية بسبب ان تنفيذها يتم عبر الشبكة المعلوماتية، وهو ما يثير في كثير من الاحيان تحديات قانونية إدارية فنية، بل سياسية بشأن مواجهتها لا سيما فيما يتعلق بإجراءات الملاحقة الجنائية (عطايا، 2010، الصفحات 374-373)

3. أنواع الجرائم الالكترونية:

إن الجريمة الإلكترونية عرفت اختلاف حول تقسيماتها، وذلك بسبب الاختلاف في تسميتها، حيث استند كل اتجاه على معيار معين، فالبعض يصنفها حسب الاسلوب المتبع في الجريمة، والبعض الاخر يستند الى دوافع ارتكابها، وآخرون يؤسسون تقسيماتهم على تعدد محل الاعتداء وتعدد الحق المعتدى عليه، أما بالنسبة للمشرع الجزائري فقد قسم الجريمة الالكترونية الى جرائم مرتكبة بواسطة النظام المعلوماتي نص عليها المشرع ولم يحددها، وبالتالي تشمل كل الجرائم المرتكبة بواسطة تكنولوجيا الاعلام والاتصال ،أما النوع الثاني من الجرائم يتمثل في الجرائم الواقعة على النظام المعلوماتي حددها المشرع بموجب قانون العقوبات ، وهذا ما سيتم بيانه في الفرعين المواليين.

1.3. الجريمة الالكترونية المرتكبة باستخدام النظام المعلوماتي:

يشمل هذا التصنيف اهم الجرائم التي تتصل بالمعلوماتية، ويعد الحاسب الالي وسيلة لتسهيل النتيجة الاجرامية ومضاعفا لجسامتها، وهي انواع منها الجريمة الواقعة على الأشخاص الجريمة الواقعة على النظم المعلوماتية الأخرى الجريمة الواقعة على الأسرار، وسنوضح كل نوع منها في البنود الاتية.

1.1.3. الجريمة الالكترونية الواقعة على الاشخاص الطبيعية: تنقسم هذه الجرائم بدورها إلى جرائم واقعة على حقوق الملكية الفردية، وجرائم واقعة على حرمة الحياة الخاصة.

- **الجريمة الالكترونية الواقعة على حقوق الملكية الفكرية:**

يكون النظام المعلوماتي وسيلة للاعتداء على حقوق الملكية الفردية، ومثاله السطو على المعلومات وتخزين واستخدام هذه المعلومات دون إذن صاحبها، لأن استخدام معلومة معينة دون اذن صاحبها يعتبر اعتداء على حق معنوي ، إضافة إلى كونه اعتداء على قيمتها المالية كون ان للمعلومة قيمة ادبية بجانب قيمتها المادية ،ويندرج ضمن الحقوق الفكرية كذلك براءات الاختراع ، اذ تمثل فكرة المخترع تحتوي على حق معنوي وأخر مالي للمخترع ، وقد نص المشرع الجزائري على حقوق الملكية الفكرية من خلال نصوص قانونية وهي الأمر رقم 03-05 الصادر في 2003 ، المتعلق بحقوق المؤلف والحقوق المجاورة، والأمر رقم 03-07 الصادر في 2003 المتعلق ببراءات الاختراع (سوير، 2011، الصفحات 14-15-16)

- **الجريمة الالكترونية الواقعة على حرمة الحياة الخاصة:**

لقد كرس المشرع الجزائري حرصه على حماية الحياة الخاصة للمواطنين وعدم الاعتداء على هذه الحرمة، ولما كان الحاسب الالي بمثابة مخزن لأهم المعلومات المتعلقة بالأفراد لقدرته على تخزين اكبر قدر ممكن من المعلومات، وهذا ما جعل للحاسب الالي دور في تسهيل الحصول على هذه المعلومات عن طريق الغير بإفشائها لتحقيق مصالح مختلفة، ومثاله أن يقوم شخص يعمل بالنظام المعلوماتي يعلم الشخص المعني ولكن يقوم المكلف بحفظها بإطلاع

الغير عليها دون اذن صاحبها، أو ان يقوم شخص باختراق معلومات هي بمثابة اسرار مكتوبة وسير ذاتية ومذكرات شخصية لشخص اخر.

2.1.3. الجريمة الالكترونية الواقعة على النظم المعلوماتية الأخرى:

تتحقق هذه الجريمة بالولوج المادي من جانب الشخص في مركز المعالجة المعلوماتية، أو استخدام اداة الكترونية معينة تسمح بالتقاط المعلومات والتصنت عليها لدى النظم المعلوماتية الأخرى بالإضافة إلى إساءة استخدام البطاقة الائتمانية.

بالنسبة للحالة الاولى المتمثلة في الولوج المادي في مركز المعالجة المعلوماتية، حيث يستطيع الجاني هذا الاستيلاء شاشة النظام ، او الاطلاع على المعلومات بقراءة ما هو مكتوب عليها، أو باستخدام مكبر الصوت . أما الحالة الثانية في حالة اساءة استخدام العميل البطاقة الائتمانية، وذلك عن طريق عدم احترام العميل المصدر اليه البطاقة الائتمانية شروط العقد الملزم بينه وبين البنك، كاستعماله بطاقة ائتمانية انتهت مدة صلاحيتها او ثم الغاؤها، أم الحالة الثالثة كما في حالة قيام سارق باستعمال بطاقة ائتمانية للحصول على السلع والخدمات (سوير، 2011، الصفحات 35-36-37).

3.1.3. الجريمة الالكترونية الواقعة على الاسرار:

تقوم هذه الجريمة باستعمال النظام المعلوماتي لإفشاء الأأسرار، سواء كانت اسرار عامة او اسرار خاصة تتعلق بالأفراد أو المؤسسات المختلفة، ويتخذ هذا النوع من الجرائم صورتين، الأولى تتعلق بالجرائم الواقعى على اسرار الدولة ، حيث اتاح الانترنت للكثير من الدول ممارسة التجسس على دول أخرى، وذلك بالإطلاع على الاسرار العسكرية والاقتصادية لهذه الاخيرة خاصة في الدول التي يكون فيها نزاعات، والثانية تتعلق بالجرائم الواقعة على الأسرار المهنية ، والهدف من ارتكاب هذه الجريمة هو سرقة معلومات قصد التشهير بشخص أو بجماعة معينة أو بيع هذه المعلومات لتحقيق مصالح مختلفة، كالحصول على عائد مادي ممن يهمه الامر او يستخدمها للضغط على أصحابها من أجل القيام بعمل او الامتناع عن القيام بعمل (سوير، 2011، صفحة 38)

وقد حرص المشرع الجزائري على حماية هذه الاسرار من خلال الباب الاول المتعلق بالجنايات والجنح ضد الشيء العمومي من المادة 61 الى المادة 96 مكرر من قانون العقوبات، بالإضافة الى المادة 394 مكرر 03 التي تنص على : " تضاعف العقوبات المنصوص عليها في هذا القسم اذا استهدفت الدفاع الوطني او الهيئات والمؤسسات الخاضعة للقانون العام، دون اخلال بتطبيق عقوبات اشد (القانون رقم 04-15 ، الصادر في 10 نوفمبر 2004 ، يعدل ويتمم الامر رقم 66/156 ، الصادر في 08 جوان 1966، المتضمن قانون العقوبات)

2.3. الجريمة الالكترونية الواقعة على النظام المعلوماتي:

من أجل سد قانون الفراغ الذي عرفه التشريع الجزائري في هذا المجال، جاء القانون رقم 04-15 الصادر في 10 نوفمبر 2004، المتضمن العقوبات بتحريم كل انواع الاعتداءات التي تستهدف انظمة المعالجة الالية للمعطيات، وقد ورد النص على هذه الجرائم في القسم السابع مكرر من قانون العقوبات، تحت عنوان المساس بأنظمة المعالجة الالية للمعطيات، وذلك في المواد 394 مكرر الى 394 مكرر 07، وتأخذ صور الاعتداء صورتين هما: الدخول والبقاء في منظومة معلوماتية، المساس بمنظومة معلوماتية، كما تضمن صور أخرى للغش.

1.2.3. جريمتي الدخول والبقاء غير المشروعان في منظومة معلوماتية:

تنص المادة 394 مكرر من قانون العقوبات السابق الذكر على معاقبة كل شخص يدخل او يبقى بواسطة استعمال الغش في كل أو جزء من منظومة المعالجة الالية للمعطيات أو يحاول ذلك، وإذا نتج عن هذا الدخول أو البقاء تخريب في النظام المعلوماتي فان العقوبة تضاعف، فالصورة البسيطة للجريمة تتمثل في مجرد الدخول او البقاء بينما الصورة المشددة تتحقق في الحالة التي ينتج فيها عن هذا الدخول أو البقاء غير المشروع أما محو او تغيير في المعطيات الموجودة في النظام (عقون، 2012، الصفحات 183-182).

أ- فعل الدخول غير المشروع: لا يعني هنا الدخول بالمعنى المادي، أي الدخول الى مكان معين كمنزل أو غيره، وإنما ينظر اليه كظاهرة معنوية تشابه تلك التي نعرفها عندما نقول الدخول إلى فكرة أو الى ملكية التفكير لدى الانسان، اي الدخول الى العمليات الذهنية التي يقوم بها نظام المعالجة الالية للمعطيات، وتقع هذه الجريمة من كل انسان ايا كانت صفته سواء كان شخص يعمل في مجال المعلوماتية أو لا يعمل، وسواء كان يستطيع ان يستفيد من الدخول أم لا فيكفي ان يكون ممن ليس له الحق في الدخول إلى النظام او من الذين ليس لهم الحق في الدخول بالطريقة التي دخلوا بها كما تقع الجريمة سواء تم الدخول الى النظام كله أو إلى جزء منه فقط، اي ان الجريمة تقوم بفعل الدخول الى النظام مجردا عن أي نتيجة اخرى، ولا يشترط لقيامها التقاط أو حصول الشخص على المعلومات الموجودة داخل النظام أو البعض منها، بل أن الجريمة تتوافر حتى ولو لم تكن لدى الجاني القدرة الفنية على تنفيذ العمليات على النظام ، ففعل الدخول يتسع ليشمل كل فنيات الدخول الاحتيالي في منظومة محمية كانت او غير محمية ، كما تشمل استعمال من لا حق له في ذلك المفتاح للدخول الى المنظومة.

ب- فعل البقاء غير المشروع: يقصد بفعل البقاء التواجد داخل نظام المعالجة الالية للمعطيات ضد ارادة من له الحق في السيطرة على هذا النظام، وقد يتحقق فعل البقاء المعاقب عليه مستقلا عن الدخول في النظام وقد يجتمعان ، ويكون البقاء معاقبا عليه استقلالا حين يكون الدخول الى النظام مشروعا، ومن أمثلة ذلك اذا تحقق الدخول الى النظام بالصدفة او عن طريق الخطأ، وهنا يجب على المتدخلأ يقتطع وجوده داخل النظام وينسحب، فإذا بقي رغم ذلك فانه يعاقب على جريمة البقاء غير المشروع، ويكون البقاء جريمة في الحالة التي يطبع الشخص فيها نسخة من المعلومات في الوقت الذي كان مسموحا له فيها الاطلاع فقط، ويتحقق ذلك أيضا بالنسبة للخدمات المفتوحة للجمهور مثل الخدمات الهاتفية، والتي يستطيع الجاني فيها الحصول على الخدمة دون ان يدفع المقابل الواجب دفعه أو يحصل على مدة اطول من المدة التي دفع مقابلها ، ففعل البقاء يشمل البقاء بعد الدخول الشرعي اكثر من الوقت المحدد، وذلك بغية عدم الدفع، كما تقوم الجريمة سواء حصل الدخول مباشرة على الحاسوب او حصل عن بعد ، كما يحرم البقاء حتى لو حصل الدخول بصفة عرضية (عقون، 2012، الصفحات 183-184)

2.2.3.جريمة المساس بالمنظومة المعلوماتية:

نصت المادة 394 مكرر 01 من قانون العقوبات رقم 04/ 15 بمعاقبة كل شخص قام بإدخال معطيات في نظام المعالجة الآلية، أو أزال أو عدل هذه المعطيات وذلك عن طريق استعمال الغش، هذا السلوك الاجرامي يتجسد في ثلاث صور هي الإدخال، المحو، التعديل، كما ان المشرع لم يشترط اجتماع هذه الصور بل يكفي ان يصدر عن الجاني احداهما فقط لكي يتوفر الركن المادي، وأفعال الادخال والإزالة والتعديل تنطوي على التلاعب في المعطيات التي يحتويها نظام المعالجة الالية للمعطيات، سواء بإضافة معطيات جديدة غير صحيحة او محو او تعديل معطيات موجودة من

قبل كما ان هذا السلوك يجسد فعل التخريب وإفساد المعطيات التي يتضمنها نظام المعالجة الالية، مثال ذلك ادخال فيروس المعلوماتية في البرامج من اجل اتلافها.

وعليه ومن خلال ما تم التطرق اليه سابقا فان هذا النمط من الجرائم له ميزة خاصة، بحيث يكون سهل حال ارتكابها ولكن شديدة الخطورة في نتائجها، وقد ترتكب أخطر الجرائم في بضعة ثواني، ودون التقاء بين الجاني والمجني عليه وهذا ما يؤدي الى صعوبة مكافحتها، والشيء الذي يعاب على المشرع الجزائري أنه أهمل المجرم الالكتروني وتسليط العقوبة عليه ولم يتعرض له في اي نص قانوني، واهتم فقط بالجريمة الالكترونية بالنص على بعض الجرائم وليس كلها.

4. دوافع ارتكاب الجريمة الالكترونية:

هناك العديد من الدوافع التي تحرك الجناة لارتكاب افعال الاعتداء المختلفة في هذا النمط من الجرائم، واهم هذه الدوافع سيتم بيانها كالأتي:

1.4. الدوافع الشخصية لارتكاب الجريمة الالكترونية: تصنف هذه الدوافع الى دوافع مادية وأخرى ذهنية، وسيتم تناوله لاحقا.

أ)- الدوافع المادية:

يعتبر الدافع المادي من اكثر الدوافع التي تحرك الجاني لاقتراف الجريمة الالكترونية، وذلك لان الربح الكبير والممكن تحقيقه من خلالها يدفع بالمجرم الالكتروني الى تطوير نفسه حتى يواكب كل جديد يطرأ على التقنية المعلوماتية ويستغل الفرص ويسعى الى الاحتراف حتى يحقق اعلى المكاسب وبأقل جهد دون ان يترك اثر ورائه، فيتعمد الجاني رغبة منه في تحقيق الربح الى التلاعب بأنظمة المعالجة الالية للبنوك والمؤسسات المالية ان كان أحد موظفيها، أو اختراق نظم المعالجة الالية من خلال اكتشافه لفجواتها الامنية، فيعمل على استغلالها وبرمجتها لتحويل مبالغ مالية لحسابه ، أو لحساب شركائه، أو لحساب من يعمل لحسابهم إن كان من خارج المؤسسة، كما يمكن الحصول على مكاسب مادية من خلال المساومة على البرامج و المعلومات المتحصل عليها بطريق الاختلاس من جهاز الحاسوب (وضاح و المجالي، 2005، الصفحات 61-62).

ب) -الدوافع الذهنية لارتكاب الجريمة الالكترونية:

تتمثل هذه الدوافع في المتعة والتحدي والرغبة في فهم النظام المعلوماتي واثبات الذات، وقد تكون هذه الدوافع مجرد شغف بالالكترونيات والرغبة في تحدي وقهر النظام والتفوق على تعقيد وسائل التقنية، فاختراق الانظمة الالكترونية وكسر الحواجز الامنية المحيطة بهذه الانظمة قد يشكل متعة كبيرة لمرتكبها وتسلية تغطي أوقات فراغه وعلى صعيد اخر قد يكون اقدام المجرم الالكتروني على ارتكاب جريمته بدافع الرغبة في قهر الانظمة الالكترونية والتغلب عليها، اذ يميل هنا الى اظهار تفوقه على وسائل التكنولوجيا الحديثة، وفي الغالب تكون لديهم دوافع حاقدة او تخريبية ، وإنما ينطلق من دافع التحدي واثبات المقدرة (سعيداني، 2013، الصفحات 61-62)

2.4. الدوافع الموضوعية لارتكاب الجريمة الالكترونية:

قد يتأثر المجرم الالكتروني ببعض المواقف قد تكون دافعة له على اقتراف الاجرام الالكتروني ولا يسعى في ذلك حينها لا للمتعة والتسلية ولا لكسب المال، ويمكن ابراز اهم الدوافع كا الاتي:

أ)- دافع الانتقام وإلحاق الضرر برب العمل :

ويتوفر هذا الدافع نتيجة فصل الموظف من عمله، أو تخطيه في الحوافز أو الترفيه، فهذه الامور تجعله يقدم على ارتكاب جريمته، كما هذا الدافع من أخطر الدوافع التي يمكن ان تدفع الشخص إلى ارتكاب الجريمة، ذلك انه غالبا ما يصدر عن شخص يملك معلومات كبيرة عن المؤسسة او الشركة التي يعمل بها، وغالبا ما يكون هذا الدافع لأسباب تتعلق بالحياة المهنية ومن ذلك الشعور بالحرمان من بعض الحقوق المهنية، أو الطرد من الوظيفة، فيتولد لدي المجرم الالكتروني الرغبة في الانتقام من رب العمل.

ب)- دافع التعاون والتواطؤ :

هذا النوع يتكرر كثيرا في الجرائم الالكترونية، وغالبا ما يحدث بالتعاون بين متخصص في الانظمة المعلوماتية اين يقوم بالجانب الفني من المشروع الاجرامي، وأخر من المحيط او خارج المؤسسة المجني عليه يقوم بتغطية عمليات التلاعب وتحويل المكاسب المادية، وعادة ما يمارسون التلصص على الانظمة وتبادل المعلومات بصفة منظمة حول انشطتهم (سعيداني، 2013، صفحة 62)

وعليه فان هذا الدوافع الخاصة بارتكاب الجريمة الالكترونية فهي غير ثابتة ومعتمدة لدى الباحثين والمختصين لان السلوك الاجرامي والدوافع لارتكاب الجريمة الالكترونية قد تتغير وتتحول بسرعة من محاولة التحدي والتغلب على الأنظمة الى تدميرها او القيام بعمليات الابتزاز او الحصول على الأموال، وعليه فان كل جريمة جديدة دوافع جديدة.

5. مظاهر تحديات الجريمة الالكترونية: يمكن ايجاز مظاهر تحديات الجريمة الالكترونية فيما يلي:

- ✓ عدم وجود اتفاق عام بين الدول على مفهوم الجرائم الالكترونية، وبالتالي عدم وجود توافق بين قوانين الاجراءات الجنائية للدول بشأن التحقيق في تلك الجرائم.
- ✓ ايضا يمثل النقص الظاهر في مجال الخبرة لدى رجال الشرطة وجهات الادعاء والقضاء تحديا كبيرا في القضاء على هذه الجريمة.
- ✓ الاعتداء على برامج ومعلومات الحاسب يجعلنا امام مشكلة قانونية ذات طبيعة خاصة سميت هذه الجريمة في فرنسا بجريمة التوصل بطريق التحايل لنظام المعالجة الالية للبيانات وهي جريمة مستحدثة.
- ✓ ظهور وتنامي الانشطة الاجرامية الالكترونية وتوسل مرتكبيها بتقنيات جديدة غير مسبوقة في مجال تكنولوجيا المعلومات والاتصالات.
- ✓ تستعصي بعض هذه الانشطة الاجرامية الالكترونية على ادراجها ضمن الاوصاف الجنائية التقليدية في القوانين الجنائية الوطنية والأجنبية.
- ✓ ظاهرة الجرائم الالكترونية باتت تتخذ انماطا جديدة وضربا من ضروب الذكاء الاجرامي وهذا بلا شك يمثل تحديا جديدا في الوقت الحاضر.
- ✓ هشاشة نظام الملاحقة الاجرامية التي تبدو قاصرة على استيعاب هذه الظاهرة الاجرامية الجديدة سواء على صعيد الملاحظة الجنائية في إطار القوانين الوطنية ام على صعيد الملاحقة الجنائية الدولية (عطايا، 2010، صفحة 375).

✓ يعد الجدل الحاصل في مسالة تخزين المعلومات او البيانات المعالجة إلكترونيا خارج اقليم الدولة من أكبر تحديات الجريمة الالكترونية حيث نتج عنه اتجاهان لمكافحة هذا النوع من الجرائم: الاتجاه الاول يرى انه من غير المشروع ان تقوم سلطات الدولة ما بالتدخل وتفتيش النظم المعلوماتية الموجودة في اقليم دولة أخرى، هدف كشف وضبط ادلة اثبات جريمة كانت قد وقعت على أراضيها، وذلك استنادا الى مبدأ اقليمية القانون.

أما الاتجاه الثاني فيتمثل في ان القانون الدولي يمكن ان يتشكل من خلال توافق الاراء على الصعيد الدولي باتجاه السماح بتنفيذ هذه الإجراءات حال توافر ظروف معينة يتم تحديدها، كإشعار الدولة المراد تفتيش البيانات والمعلومات المخزنة بنظمها المعلوماتي.

6. آليات مواجهة الجريمة الالكترونية:

1.6. الأجهزة العملياتية المختصة في مكافحة الجرائم الالكترونية:

1.1.6. من الناحية القانونية:

✓ **الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها:**

تشكلت هذه الهيئة بمقتضى المرسوم الرئاسي رقم 15-261 وهي سلطة إدارية مستقلة لدى وزير العدل، تعمل تحت إشراف ومراقبة لجنة مديرية يترأسها وزير العدل وتضم أساسا أعضاء من الحكومة معنيين بالموضوع ومسؤولي مصالح الأمن وقاضيين من المحكمة العليا يعينهما المجلس الأعلى للقضاء. (عبان، 2016، صفحة 91)

وكلفت الهيئة باقتراح عناصر الإستراتيجية الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها وتنشيط وتنسيق عمليات الوقاية منها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في مجال مكافحة هذه الجرائم، من خلال جمع المعلومات والتزويد بها ومن خلال الخبرات القضائية، وضمان المراقبة الوقائية للاتصالات الإلكترونية، قصد الكشف عن الجرائم المتعلقة بالأعمال الإرهابية والتخريبية والمساس بأمن الدولة.

وقد نص سابقا على إنشاء هذه الهيئة المادة 13 من القانون 09/04 المؤرخ في أوت المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها من خلال: " **تنشأ هيئة وطنية وتنظيمها وكيفيات سيرها عن طريق التنظيم"** أما مهامها فقد أوردتها المادة 14 من نفس القانون وتتمثل في: (عطية، صفحة 04) (بارة، دون سنة ، صفحة 445)

أ-الوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال: إن إجراءات الوقاية تكون بتوعية مستعملي تكنولوجيات الإعلام والاتصال بخطورة الجرائم التي يمكن أن يكونوا ضحاياها وهم يتصفحون أو يستعملون هذه التكنولوجيات، ومن أهم هذه الجرائم: التجسس على الاتصالات والرسائل الالكترونية، التلاعب بحسابات العملاء، اختراق أجهزة الشركات والمؤسسات الرئيسية أو الجهات الحكومية...الخ.

ب-مكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال: بحسب نص المادة 14 من القانون 09/04 هناك نوعان من المكافحة تقوم بهما هذه الهيئة:

✓ مساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن الجرائم المتصلة بتكنولوجيا الإعلام والاتصال بما في ذلك تجميع المعلومات وإنجاز الخبرات القضائية المادة 14 فقرة (ب) من القانون 09/04.

✓ تبادل المعلومات مع نظيراتها في الخارج قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها(CRAIYEN AND OTHERS,2014,P14) يقترح المشروع في هذا الفصل إنشاء هيئة وطنية مختصة تتولى مهام أهمها : تنشيط وتنسيق عملية الوقاية من الجرائم المعلوماتية ومساعدة السلطات القضائية ومصالح الشرطة القضائية من التحريات التي تجريها بشأن هذه الجرائم، وما تقوم به أيضا من تجميع المعلومات من نظيرتها في الخارج قصد محاربة هذا النوع الخطير من الإجرام (بارة، دون سنة ، صفحة 445)

2.1.6.من الناحية العلمية:

المصلحة المركزية لمكافحة الجريمة المعلوماتية -DGSN– (SCLC):

استجابة لمطلب الأمن المعلوماتي ومحاربة التهديدات الأمنية الناجمة عن الجرائم السيبرانية قامت مصالح الأمن بإنشاء المصلحة المركزية للجريمة الإلكترونية التي عملت على تكييف التشكيل الأمني لمديرية الشرطة القضائية، والتي كانت عبارة عن فصيلة شكلت النواة الأولى لتشكيل أمني خاص لمحاربة الجريمة السبرانية وعلى مستوى المديرية العامة للأمن الوطني والتي أنشئت سنة 2011 ليتم بعدها إنشاء المصلحة المركزية لمحاربة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال بقرار من المدير العام للأمن الوطني وأضيف للهيكل التنظيمي لمديرية الشرطة القضائية في جانفي 2015 (عرابة و النعيم، 2016، صفحة 130)

✓ **مركز الوقاية من جرائم الإعلام الآلي للدرك الوطني(CPLCIC):**

وقد أنشئ في سنة 2008 ويعتبر الجهاز الوحيد المختص بهذا الصدد في الجزائر، وهدف إلى تأمين منظومة المعلومات لخدمة الأمن العمومي، واعتبر بمثابة مركز توثيق ومقره يوجد ببئر مراد رايس، وهذا المركز يعكف على تحليل معطيات وبيانات الجرائم المعلوماتية المرتكبة، وتحديد هوية أصحابها سواء كانوا أشخاص فرادى أو عصابات، وهذا كله من أجل تأمين الأنظمة المعلوماتية والحفاظ عليها، لاسيما تلك المستعملة في المؤسسات الرسمية وللبنوك (روابحي، 2010، صفحة 78)

ويهدف هذا المركز إلى مساعدة الأجهزة الأمنية الأخرى بالتعاون من أجل مكافحة الجرائم المعلوماتية، حيث يعنى المركز بتطوير أساليب التعامل مع هذه الجرائم ووضع قوانين لتنظيم مجال استغلال المعلومة من خلال تنسيق مع وزارة العدل ومعهد خاص بعلم الإجرام لتطوير مستوى التعامل مع الجريمة بصفة عامة والجريمة المعلوماتية بصفة خاصة، فالجزائر تعمل جاهدة على الاستفادة من خبرات البلدان الأخرى في تأمين المنظومة المعلوماتية وحمايتها من الجرائم ضمن مجموعة من العناصر أهمها (علوي، 2008، صفحة 41)

- **الوقاية:** وتشمل حملة تحسيسية وتوعية بالتنسيق مع وزارة التضامن الوطني والأسرة والعمل على ملتقيات ومحاضرات وأياما دراسية ومنتديات دولية، ومشاركة في منتديات صحفية وحصص تلفزيونية وإذاعية وغيرها من وسائل النشر والإشهار.
- **المكافحة:** توعية الجزائريين من خلال استعمالهم لشبكات التواصل واستخدام الانترنت وذلك من خلال تعليقاتهم المدافعة عن الجزائر ومعرفة الأخطار بسلوكيات مشبوهة أو اعتداءات عبر نشر فيديوهات توصل إلى الجناة، مما يسهل التحقيق لدى مصالح الدرك وإلقاء القبض على المشبوهين ومرتكبي الجرائم في الوقت المناسب.

✓ **المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني(INCC):**

مؤسسة عمومية ذات طابع إداري تحت الوصاية المباشرة لوزير الدفاع الوطني مكلفة بمهام متعددة كإجراء الخبرات والفحوص في إطار التحريات الأولية والتحقيقات القضائية، ضمان المساعدة العلمية أثناء القيام بالتحريات المعقدة (كريم، 2008، صفحة 36)

يعتبر المعهد أحد المشاريع المنجزة في إطار تطوير سلك الدرك الوطني" ببوشاوي" ، حيث تم إنشاءه بموجب مرسوم رئاسي 133/04 المؤرخ في 26 جوان 2004 ،ودخل حي المورد البشري واقتناء المعدات العلمية والتقنية الضرورية، ويقوم المعهد بالعديد من مهامً الخدمة ابتداء من الفاتح جانفي 2009 ،أما الفترة الممتدة بين 2004 و2009 كرست للتكوين التي من شأنها تلبية الطلبات الواردة من السلطة القضائية ، ضباط الشرطة القضائية والسلطات المؤهلة، قانونيا خاصة أثناء معالجة القضايا المعقدة (ربه، 2006، الصفحات 33-34-35)

والإسهام في تنظيم دورات الإتقان والتكوين ما بعد التدرج في تخصص العلوم الجنائية ، ولتأدية مهامه على أكمل وجه فإن المعهد الوطني للأدلة الجنائية وعلم الإجرام يحتوي على العديد من الأقسام والمصالح المختصة من أهمها: مصلحة البصمات؛ مصلحة البيئة؛ أما في ما يخص مجال الأمن السيبراني هناك مصلحة الإعلام الآلي؛ على مستوى هذه المصلحة يتم رصد ومراقبة وتتبع عمليات الاختراق والقرصنة المعلوماتية وكذا اكتشاف المعلومات المسروقة وتفكيك البرامج المعلوماتية (غزال، 2014، صفحة 64)

7. خـاتـمـة:

في السنوات الاخيرة اصبح الكمبيوتر والانترنت محرك عجلة التنمية ووسيلة الرقي والتقدم في كافة العلم، كما تعتبران هاتان الوسيلتان كاتمتان لأسرار عدة قطاعات ووسيلة تواصل رئيسية عبر العالم، الا انهما في نفس الوقت اصبحتا للأسف وسيلة ارتكاب أخطر الجرائم العابرة للدول والقارات ألا وهي الجرائم الإلكترونية، ولهذا يتطلب مكافحة الجرائم الالكترونية من خلال وضع سياسة وطنية ودولية محكمة تفرض عقوبات صارمة ورادعة على مرتكبي جرائم الانترنت، كما يستوجب الاعتماد على أساليب وتقنيات متطورة لحماية قطاع المعلوماتية والتمكن من الكشف عن مرتكبي هذه الأفعال غير المشروعة.

إن من اهم التحديات التي تواجه المشرع هو موضوع التجريم والعقاب، اذ يتوجب على المشرع في كافة الدول التي لا تشتمل قوانينها على نصوص تجرم الجرائم الالكترونية المبادرة الى ذلك في الحين، كما نجد بالمقابل ان معظم الجرائم الالكترونية مصنفة في كثير من الدول على انها جنح ، بالرغم من خطورتها وشدة جسامتها، لكن هذه النظرة بدأت تتغير مؤخرا وذلك مع نمو ظاهرة الجريمة الالكترونية وتشعبها، وكذلك بسبب انشاء اقسام خاصة بملاحقة هذه الجرائم والتحقيق فيها والتي ساهمت بدورها ايجابيا في زيادة الوعي بخطورة هذا النوع من الجرائم.

الـتـوصـيـات: يمكن وضع مجموعة من التوصيات وهي كالتالي:

1-تعديل قانون العقوبات ليشتمل على تجريم الجرائم الالكترونية، أو سن قانون مكافحة الجرائم الالكترونية.

2-تغليظ عقوبة الجرائم الالكترونية، واعتبار خطورة الجريمة، بتهديدها للأمن الداخلي والعالمي وحجم الضرر، من الظروف المشددة للعقوبة التي ترفع مستوى الجريمة لتصبح جناية.

3- عدم فتح اي رسالة الكترونية من مصدر مجهول، لان مرتكبي الجرائم الالكترونية يستخدمون وسائل البريد لالكتروني، لإرسال ملفات التجسس على الضحايا.

4-وضع ارقام سرية على الملفات المهمة حيث لا يستطيع فتحها سوى من يعرف الرقم السري فقط، ومحاولة تغيير كلمة السر باستمرار فهي قابلة للاختراق.

5-تطوير قدرات التقنية على شبكة الانترنت، وإنشاء شرطة الانترنت للقبض على مرتكب الجرائم حال دخولهم على الشبكة من خلال التتبع الفني للجهاز او الخط الهاتفي الذي ارتكبت منه الجريمة.

6-العمل على انشاء محاكم للقضايا الافتراضية على شبكة الانترنت لتتمكن من التعامل مع هذه الانواع المستحدثة من الجرائم.

7-جعل القرصنة على البرامج بمثابة جريمة سرقة، مثلها مثل سرقة اي سلعة اخرى.

8-الاحتفاظ بنسخ احتياطية لكل المعلومات الحساسة في اقراص اضافية ليست مرتبطة بالشبكة.

9-ضرورة استخدام بعض البرامج (مكافحة الفيروسات) التي صممت خصيصا للكشف والوقاية من الفيروس والبعد عن استعمال كلمة السر البسيطة.

10-العمل على تنمية الكوادر البشرية العاملة في مجالات مكافحة الجرائم الالكترونية.

11-تسليط الضوء على علم النفس السيبراني من أجل العمل على اكتشاف آليات جديدة في التنبؤ بتحراكات المهاجم السيبراني داخل الفضاء السيبراني وخارجه.

12-محاولة اكتشاف المخترق الالكتروني عن طريق تحليل شخصيتة وإعادة احتواءه وتأهيله حتى يتم الاستفادة من كفاءته باعتباره على درجة كبيرة من الخطورة الإجرامية.

13-تكثيف دراسة العوامل النفسية المتسببة في تكوين المهاجم السيبراني ونزعها من جذورها قبل نموها في المجتمعات.

14-تفشي الجرائم السيبرانية وتنوعها وتعدد أشكالها وتمرس فاعليها في ارتكابها مما يحتاج إلى تطوير التشريعات القانونية الخاصة بمثل هذه الأفعال وهذا تماشيا مع التطورات الحاصلة في عالم التكنولوجيا.

15-تنظيم دورات تكوينية في تطوير المناهج المتقدمة لحماية سرية البيانات والأنظمة المعلوماتية من الهجوم السيبراني، وهذا يكون بالاستغلال الجيد لثورة المعلومات وفق المواصفات الدولية التي أوصت بها علامة أيزو والاتحاد الدولي للاتصالات مع إشراك كل الفاعلين في المجال الأمني.

16-إيلاء الجانب التقني أهمية كبرى على مستوى مكافحة الجريمة الإلكترونية من خلال اعتماد تقنية التشفير بشكل أوسع في المعاملات الإلكترونية وفي المواقع الإلكترونية التي لها علاقة بالأمن الوطني.

17-إحداث هيئة خاصة لمكافحة الجرائم الالكترونية تتكون من مهندسين مختصين في مجال المعلوماتية، مع السماح لهم قانونيا باعتماد وسائل استقصاء وتعقب خاصة مثل استعمال أسماء مستعارة في منتديات الانترنت قصد تحديد هوية المجرمين دون أن يكونوا مسؤولين جزائيا.

18-الاستثمار في مجال الأمن السيبراني من خلال توطين التكنولوجيا والبني التحتية السيبرانية، والثاني تطوير المهارات والخبرات في سبيل امتلاك قدرات وطنية قادرة على بناء وإدارة وتحليل الأنظمة السيبرانية وتطويرها.

19-التنسيق مع مختلف دول العالم من أجل التصدي للجريمة السيبرانية مع التفكير بجدية في إدراج مجال الفضاء السيبراني ضمن مناهج التعليم في الدول العربية عموما وفي الجزائر خصوصا.

قائمة المراجع:

1) ابراهيم رمضان ابراهيم عطايا. (2010). *الجريمة الالكترونية وسبل مواجهتها في الشريعة الاسلامية والا نظمة الدولية* (دراسة تحليلية تطبيقية). القاهرة : دون دار نشر .

2) اسامة بن صادق عطية. (بلا تاريخ). الحكومة الالكترونية (نحو مجتمع المعرفة). معهد البحوث والاستشارات(العدد التاسع).

3) التنظيم القانوني والجرائم الالكترونية (مابين امن المعلومات وتقييد الحريات). (2018). القاهرة: مركز هردو لدعم التعبير الرقمي .

4) - القانون رقم 04-15 ، الصادر في 10 نوفمبر 2004 ، يعدل ويتمم الامر رقم 66/156 ، الصادر في 08 جوان 1966، المتضمن قانون العقوبات. (بلا تاريخ).

5) القانون رقم 04-15 ، الصادر في 10 نوفمبر 2004 ، يعدل ويتمم الامر رقم 66/156 ، الصادر في 08 جوان 1966، المتضمن قانون العقوبات ، جر، العدد 71. (بلا تاريخ).

6) بن عبد ربه. (2006). النظام الاقتصادي الجديد المبني على المعرفة وتطور مجتمع المعلومات والتكنولوجيا الحديثة للاتصال (الحلول المقترحة لارساء مجتمع المعلومات ناجح ومتكامل في الجزائر) . رسالة ماجستير. الجزائر، كلية العلوم -السياسية والاعلام -جامعة الجزائر-.

7) حمزة بن عقون. (2012). السلوك الاجرامي للمجرم المعلوماتي . مذكرة ماجستير في العلوم القانونية تخصص علم الاجرام وعلم العقاب. باتنة ، جامعة الحاج لخضر .

8) خيرة روابجي. (2010). ثقافة الانترنت (دراسة ميدانية لاستعلامات الشبكة بمدينة تيهرت. رسالة ماجستير . وهران ، كلية العلوم الانسانية والحضارة الاسلامية (قسم علم المكتبات والعلوم الوثائقية .

9) سعيداني نعيم. (بلا تاريخ). اليات البحث والتحري عن الجريمة المعلوماتية في القانون الجزائري. مذكرة ماجستير في العلوم القانونية تخصص علوم جنائية . جامعة الحاج لخضر، باتنة : 2013.

10) سميرة بارة. (دون سنة). الدفاع الوطني والسياسات الوطنية للامن السيبيراني في الجزائر: الدور والتحديات . ورقلة : جامعة قاصدي مرباح .

11) سوير سفيان. (2011). جرائم المعلوماتية. مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الاجرام. جامعة ابو بكر بلقايد ، تلمسان.

12) شاهد الياس عرابة، و دفرو عبد النعيم. (2016). تقييم تجربة تطبيق الحكومة الالكرونية في الجزائر. المجلة الجزائرية للدراسات المحاسبية والمالية(العدد الثالث).

13) عادل غزال. (2014). مشاريع الحكومة الالكترونية من الاستراتيجية الى التطبيق، مشروع الجزائر ، الحكومة الالكترونية-انموذجا-. مجلة المكتبات والمعلومات(العدد 34).

14) عبد القادر عبان. (2016). تحديات الادارة الالكترونية في الجزائر (دراسة سوسيولوجسة ببلدية الكاليتوس العاصمة). اطروحة دكتوراه ل م د . بسكرة ، جامعة محمد خيضر (كلية العلوم الانسانية والاجتماعية).

15) مجدي علي العريان. (2004). الجرائم المعلوماتية. الاسكندرية: دار الجامعة الجديدة.

16) محمود الحمود وضاح، و نشات نفضي المجالي. (2005). جرائم الانترنت (التعرض للاخلاق والاداب العامة ، الحض على الفجور ، جرائم الاسنغلال الجنسي للاطفال). عمان ، الاردن : دار المنار.

17) مراد كريم. (2008). مجتمع المعلومات واثرها في المكتبات الجامعية -مدينة قسنطينة انموذجا-. اطروحة دكتوراه . قسنطينة ، كلية العلوم الانسانية والاجتماعية -جامعة قسنطينة-.

18) هند علوي. (2008). المرصد الوطني لمجتمع المعلومات الجزائري (قياس النفاذ على تكنولوجيا المعلومات بقطاع التعليم بالشرق الجزائري). اطروحة دكتوراه. قسنطينة ، كلية العلوم الانسانية -جامعة منتوري قسنطينة-.

19) وضاح محمود الحمود، نشات نفضي المجالي. (2005). جرائم الانترنت (التعرض للاخلاق والاداب العامة، الحض على الفجور ، جرائم الاستغلال الجنسي للاطفال). عمان ، الاردن: دار المنار.

الصعوبات التي يثيرها الاثبات في الجرائم الالكترونية

Difficulties posed by Evidence In Cybercrime

ط.د.عبد الإله معداد/ كلية العلوم القانونية والسياسية سطات/ المغرب.

PhD .Abdelilah Mouadad /Faculty of Sciences Legal and Political, Settat/ Morocco.

ملخص الدراسة:

إن الحديث عن الجرائم الناشئة عن الاستخدام غير المشروع للكمبيوتر كأداة لارتكاب الأفعال غير المشروعة وشبكة الانترنت المرتبطة به التي ساهمت إلى حد كبير إلى انتشار الجريمة بمختلف أشكالها، وهي ظاهرة إجرامية ذات طبيعة خاصة تتعلق بالقانون الجنائي المعلوماتي، سواء من حيث محل الجريمة أو أسباب ارتكابها أو الصعوبات التي تجابه مسألة إثباتها وهذه الأخيرة تعد من أهم الإشكالات التي ثارت في خصوص هذا الموضوع من خلال إخضاعها لقانون العقوبات وبعض القوانين التقليدية والخاصة.

Abstract:

Talking about crimes arising from the illegal use of computers as a tool for committing illegal acts and the Internet associated with it, which contributed greatly to the spread of crime in its various forms, and it is a criminal phenomenon of a special nature related to informational criminal law, whether in terms of the location of the crime or the reasons for its commission or The difficulties that face the issue of proving it, and the latter is one of the most important problems that have arisen in this regard by subjecting it to the Penal Code and some traditional and special laws.

مقدمة:

شهدت البشرية في العقود الأخيرة ثورة في مجال المعلومات، بحيث غدت وسيلة العالم نحو الرقي الحضاري والاقتصادي، وشكل الوصول إلى المعلومات رهانا رئيسيا للإنسان لارتباطها بمختلف مجالات النشاط الإنساني وجوانب الحياة المعاصرة، إذ أصبح توفيرها وحسن استغلالها من المقومات الضرورية لدفع عجلة تقدم الأمم والمجتمعات، وصار وجودها دعامة أساسية لجهود التنمية والتحديث والرقي المعرفي، كما أن الوعي بأهميتها أضحى مؤشرا ومقياسا على تقدم الدول.

ومن ثم واكب هذا التوسع في استعمال التقنيات ارتفاع موازٍ في أرقام الإجرام المرتكب بواسطتها، وهو ما يصطلح عليه بالجرائم الإلكترونية، الأمر الذي أثر على حقوق الأفراد وحرياتهم حيث وفرت الأنظمة الإلكترونية وسيلة جديدة في أيدي مجرمي الإلكترونية لتسهيل ارتكاب العديد من الجرائم، مما خلق تحديات كثيرة في مواجهة النظام القانوني القائم في العديد من الدول وخاصة في مواجهة القانون الجنائي، الأمر الذي دعا الفقه والقضاء إلى البحث فيما إذا كانت النصوص القائمة كافية لمواجهة هذه الجرائم بشتى أنواعها أم أن الأمر يستدعي استحداث قوانين أو نصوص خاصة قادرة على احتوائها ومراعاة طبيعتها وخصوصيتها، كما أنه لا جدال في أن الجرائم الإلكترونية أضحت أخطر وأعقد الجرائم باعتبارها عابرة للحدود، تستخدم فيها أحدث التقنيات وتتميز بانتشار مرتكبيها في أغلب الأحيان عبر

دول مختلفة، بحيث فقدت الحدود الجغرافية كل أثر في الفضاء الشبكي المتشعب العلاقات، وأصبحنا بالتالي أمام جرائم عابرة للحدود تتم في فضاء إلكتروني معقد عبارة عن شبكة اتصال لامتناهية غير مجسدة و غير مرئية متاحة لأي شخص حول العالم وغير تابعة لأي سلطة حكومية، يتجاوز فيها السلوك المرتكب المكان بمعناه التقليدي، له وجود حقيقي وواقعي غير محدد المكان.

ومنذ أن وجدت منظومة الحوسبة وتقنياتها وما بلغته من الذروة في مرحلة التشبيك المعلوماتي الاتصالي الذي ربط ملايين الحواسيب بشبكات انسابت من خلالها المعلومات والأفكار والتراث الإنساني وما ترتب عليه من زيادة أهمية المعلومة وصيرورتها أساسا للثروة المعاصرة بشكل أظهر أقصى طاقات الرقي وجعل الإبداع الذهني في أقصى درجات قوته، الذي حفز الأداة الإنسانية التنظيمية (القانون) للتحرك نحو تنظيم الروابط الاجتماعية الناجمة عن هذه المنظومة وإسباغ الحماية اللازمة للمصالح الإنسانية المترتبة عليها، ولعل أعلى درجات الحماية التي انصبت على الفكر والإبداع وثماره كانت بالوسيلة الجنائية فاستنفر القانون هذه الوسيلة لحماية ذلك الإبداع في العصر الالكتروني متجسدا في حماية المصنفات الذهنية الالكترونية بالنص الجنائي والتهديد بالعقوبة الجزائية ضد أي شكل من أشكال العدوان عليها مساسا بالحقوق القانونية المقررة على هذه النوعية الجديدة من المصنفات.

وتتعاظم خطورة الجرائم الإلكترونية يوما بعد يوم خاصة كونها أضحت تمس المصنفات الرقمية الجديدة في مجالي الكمبيوتر والانترنت، وذلك بسبب ما أتاحته هذه التقنية من سهولة الاعتداء عليها، فالتطور المعلوماتي والطفرة العلمية في مجال الحاسب الآلي اسفرت عن ظهور جرائم جديدة لم تكن معروفة لدى المجتمع في وقت سابق، وبالتالي فبقدر ما انتفع العالم بالتكنولوجيا الحديثة، بأن سهلت له الحصول على المعلومة والاطلاع على المستجدات العلمية والفكرية بقدر ما نتج عنها أفعال غير قانونية يرفضها المنطق والعقل والأخلاق، وشكلت تهديدا مستمرا ومفاجئ قد لا يعلمه الضحية إلا بعد فوات الأوان ويتوه المستهلك بين الأصل والمقرصن وكيف السبيل إلى معرفة ذلك.

أولا: أهمية الموضوع.

إن أهمية البحث في موضوع آليات مكافحة الجريمة الالكترونية في الفضاء السيبيراني، تنبع بالخصوص من الخطورة التي أصبحت تشكلها الجريمة الالكترونية وما يرتبط بها من انتهاكات لحقوق الأفراد في الخصوصية في الفضاء السيبراني. وعليه تتمثل أهمية هذا الموضوع من الناحية القانونية والاقتصادية والاجتماعية تباعا على الشكل التالي:

الأهمية القانونية:

أضحت البيئة الافتراضية تثير العديد من الإشكالات القانونية والتقنية بالرغم من الاهتمام الكبير الذي يوليه المشرع العربي لتنظيمها، مما يجعل من الأهمية القانونية لهذا الموضوع تنبع في تبيان مدى تأثير الجرائم المستحدثة على العديد من المفاهيم في مجال القانون الجنائي نظرا لظهور مفاهيم ذات طبيعة خاصة تتمثل أساسا في المعطيات والمعلومات والبيانات ذات الطبيعة غير المادية.

الأهمية الاقتصادية:

نتيجة للتطور في مجال الالكترونية، ضعفت قدرة المراقبة والتحكم وازدهرت عمليات التجسس على المعلومات المعالجة آليا وسرقتها بشكل ملفت للنظر، الشيء الذي أصبح معه هذا النوع من الإجرام يشكل خطورة بالغة على الاستثمارات سواء المحلية أو الدولية، وبالنظر لارتباط الدول فيما بينها إلكترونيا عبر الشبكة العنكبوتية تبرز على الخصوص ظاهرة القرصنة والقدرة على اختراق النظم الالكترونية والاعتداء على سرية وسلامة المعلومات، وبالتالي فمن شأن الاهتمام الدولي بمكافحة الجريمة الالكترونية أن يتجاوز كل هذه الإكراهات التي تواجه الاستثمار الرقمي

الأهمية الاجتماعية:

ترتب عن الثورة الهائلة في مجال تكنولوجيا المعلومات، أن أصبح العالم يعيش حياة زاخرة بالاتصالات السريعة ونقل المعلومات عبر المعمور، والتعامل مع نظم متقدمة للخبرة والذكاء الاصطناعي، خاصة فيما يتعلق بتعاملات البنوك الإلكترونية من سحب للأرصدة وإيداع عن طريق البطائق المغنطة، ومن ثم وجب العمل على توفير آليات ووسائل تقنية وفنية لتأمين بياناتهم الشخصية، وتنويرهم، مما يبث الثقة في نفوسهم وتشجيعهم بالإقبال على المعاملات الإلكترونية وبالتالي ازدهار هذه الأخيرة.

ثانيا: الإشكالية:

ما مدى قدرة وسائل الاثبات المستحدثة في مكافحة الجريمة الالكترونية على مستوى الدول العربية؟

ولمعالجة الإشكالية أعلاه، سوف نعمل على مناقشتها من خلال التصميم التالي:

المحور الأول: شروط قبول الدليل الإلكتروني في الميدان الجنائي ودور القاضي في تقديره.

المحور الثاني: مظاهر صعوبات الاثبات في الجريمة الالكترونية

المحور الأول: شروط قبول الدليل الإلكتروني في الميدان الجنائي ودور القاضي في تقديره

المستقر عليه في مجال الإثبات الجنائي أن القاضي لا يمكنه إصدار الأحكام وفقا لعلمه الشخصي، فإحاطته بوقائع الدعوى يجب أن يتم من خلال ما يطرح عليه من أدلة إثبات، من هنا تظهر قيمة الدليل حيث يعد العنصر الأساسي الذي ينظر من خلاله القاضي الجنائي للواقعة موضوع الدعوى، ويبني على أساسه قناعته في ثبوت التهمة عن المتهم من عدمها. ومع ذلك فوجود دليل يثبت وقوع الجريمة ونسبتها إلى شخص معين لا يكفي للأخذ به، بل ينبغي أن تكون لهذا الدليل قيمة قانونية في المشروعية واليقينية حتى يتمتع بقوته الثبوتية أمام القضاء.

وفي الجرائم الإلكترونية أبدى كل من الفقه والقضاء مخاوف كبيرة حيال الدليل الإلكتروني بسبب إمكانية عدم تعبيره عن الحقيقة، نظرا لما يمكن أن تخضع له طرق الحصول عليه من التعرض والتزييف والتحريف، وهو ما يثير مسألة مشروعية الأخذ به، إذ يشترط في الدليل الجنائي بوجه عام أن يكون مشروعا في طريقة تحصيله، كما يجب أن يكون غير قابل للشك.

وللحديث أكثر عن ذلك سنتناول شروط قبول الدليل الإلكتروني (أولا)، في حين نخصص الحديث عن دور القاضي الجنائي في تقدير الدليل الإلكتروني (ثانيا).

أولا: شروط قبول الدليل الإلكتروني.

لكي تكون للدليل الإلكتروني قوة ثبوتية ولقبوله كأساس تشيد عليه الحقيقة في الدعوى الجنائية سواء أكان الحكم الصادر فيها بالإدانة أم بالبراءة، فإنه يلزم أن تتوافر فيه الشروط الآتية:

أ: أن تتم عملية الحصول على الدليل الإلكتروني بطريقة مشروعة:

يقصد بمشروعية الدليل من حيث التحصيل، أن تتم عملية البحث عن دليل الإدانة وتقديمه للقضاء من طرف القائمين بالبحث والتحقيق وفقا للقواعد والإجراءات التي رسمها القانون، لذلك فمشروعية الدليل تقتضي أن يكون ذلك الدليل تم الحصول عليه بطرق مشروعة تدل على الأمانة والنزاهة، فمتى كان الأمر ذلك، كانت المشروعية حدا فاصلا بين حق الدولة في توقيع العقاب لضمان أمن واستقرار المجتمع وبين حق الأفراد في ضمان حقوقهم وحرياتهم الأساسية. (جمال، 2018)

وعليه فإنه وطبقا لمبدأ الشرعية الإجرائية والتي يتحصل من خلالها الدليل، لا يكون مشروعا ومن ثمة مقبولا في عملية الإثبات والتي من خلالها يتم إخضاعه للتقدير، إلا إذا جرت عملية البحث عنه أو الحصول عليه، بالطرق التي رسمها القانون والتي تكفل تحقيق توازن عادل بين حق الدولة في العقاب وحق المتهم في توفير ضمانات لاحترام كرامته الإنسانية (محمد، 2006)، و من تم يتضح أن مشروعية الدليل الجنائي تستلزم ضرورة أن يكون الإجراء المستمد منه الدليل مشروعا، وعلى هذا الأساس، فعملية جمع الأدلة إذا خالفت الأحكام والمبادئ الإجرائية التي تنظم طريقة الحصول عليها تكون باطلة، وبالتالي بطلان الدليل المستمد منها عملا بقاعدة "ما بني على باطل فهو باطل " (مختاري، 2014)، وترتيبا على ذلك فلا يجوز للقاضي القبول بدليل الكتروني تم الحصول عليه من إجراء التسرب جرى القيام به دون مراعاة الشروط الشكلية والموضوعية للإذن بمباشرة هذا الإجراء، أو كان الدليل متحصلا عليه عن طريق إكراه المتهم المعلوماتي على فك شفرة أو الإفصاح عن كلمة السر اللازمة للولوج إلى الملفات المخزنة داخل النظم الإلكترونية، أو القيام بإجراء التنصت عن بعد دون إذن من قاضي التحقيق أو من الوكيل العام للملك، لأن الدليل المتحصل وفق الطرق السابقة يكون باطلا وفاقدا للمشروعية.

وفي إطار تكريس إلزامية احترام مبدأ مشروعية الدليل الإلكتروني فقد جسدت التطبيقات القضائية المقارنة هذا التوجه عدة مرات، إذ أصدرت محكمة النقض الفرنسية قرارا انتقدت فيه حكم إدانة السلطات القضائية الفرنسية لمواطن فرنسي بجريمة الاستغلال الجنسي للأطفال عبر الأنترنت بناءا على معلومات محصلة من طرف السلطات الأمريكية، بعدما لاحظت بأن موقع المجرم تم إنشاءه من طرف مصالح شرطة نيويورك الخاصة بمكافحة هذا النوع من الجرائم، واعتبرت أن الأدلة ليست مشروعة لأنها وقعت نتيجة تحريض، وهو إجراء غير مرخص به في القانون الفرنسي، وبما أن التحريات تمت وفقا لخدعة من طرف السلطات الأمريكية للإيقاع بالمجني عليه، فلا يمكن

اعتبارها قد رعت مبدأ المشروعية، وعليه فالمتابعة يتم إلغاؤها بالرغم من تحقق إدانة المتهم بالجريمة المنسوبة إليه (هرجة م.، 1992).

وهذا فإن مشروعية الدليل مطلوبة في حالة الإدانة فقط، حيث يذهب أحد الفقهاء (هرجة، 1999) إلى القول بأنه ليس ثمة ما يمنع من تأسيس حكم البراءة على دليل غير مشروع وذلك انطلاقا من مبدأ الزامية البراءة باعتبارها هي الأصل. وهو نفس الاتجاه تبنته محكمة النقض المصرية حينما قضت بأنه " وإن كان يشترط في دليل الإدانة أن يكون مشروعا فلا يجوز أن تبنى إدانة على دليل باطل في القانون إلا أن المشروعية بشرط واجب في دليل البراءة، ذلك لأنه من المبادئ الأساسية في الإجراءات الجنائية أن كل متهم يتمتع بقرينة البراءة إلى أن يحكم بإدانته بحكم بات وأنه إلى أن يصدر هذا الحكم له الحرية الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى".

ب: يجب أن تكون الأدلة الالكترونية يقينية

يشترط في الأدلة المستخرجة من الحاسوب أن تكون غير قابلة للشك حتى يمكن الحكم بالإدانة، ذلك أنه يجب على القاضي افتراض البراءة في جميع مراحل الدعوى ولا مجال لدحضها وافتراض عكسها إلا عندما يصل اقتناع القاضي إلى حد الجزم واليقين، وهذا ما أكدته محكمة النقض في قرارلها حيث جاء فيه:" يجب أن تبنى الأحكام على الجزم واليقين لا على الشك والتخمين، ولهذا يتعرض للقض الحكم الصادر بالإدانة في حين أن المحكمة صرحت بأنه لم يوضع بين يديها دليل مادي قاطع يثبت الجريمة"، ويتم الوصول إلى ذلك عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال التمعن والتدقيق فيما يعرض عليه من وقائع الدعوى وأدلة الكترونية على اختلاف أشكالها، وما ينطبع في ذهنه من تصورات واحتمالات ذات درجة عالية من التأكيد بالنسبة لها، وهكذا يستطيع القاضي أن يحدد قوتها الاستدلالية على صدق نسبة جريمة من الجرائم الالكترونية إلى شخص معين من عدمه (جمال، 2018)، وحتى يتحقق اليقين للأدلة الالكترونية أكثر ينبغي إخضاعها للتقييم الفني بوسائل فنية من طبيعة هذا الدليل تمكن من فحصه للتأكد من سلامته من العبث أو من التغيير، وهذا فمثلما يخضع الدليل الإلكتروني لقواعد وإجراءات معينة تحكم طرق الحصول عليه، فإنه يخضع كذلك لقواعد أخرى تحكم على قيمته الثبوتية من الناحية العلمية، ولعل من أهم هذه الوسائل ما يلي:

1. تقييم الدليل الإلكتروني في سلامته من التغيير: إن الطبيعة التقنية للدليل الالكتروني تجعله في الغالب عرضة للشك في سلامته، وذلك راجع إلى إمكانية تعرضه للعبث والخروج به على نحو يخالف الحقيقة، ولأجل التأكد من سلامة الدليل الالكتروني من التغيير أو العبث يتم الاستعانة عادة بمجموعة من الآليات التالية:

1.1. تقنية التحليل التناظري الرقمي: وهي تقنية يتم من خلالها مقارنة الدليل الرقمي المقدم أمام القضاء بالأصل المدرج بالآلة الرقمية، ومن ثمة يتم التأكد من مدى حصول تغيير في النسخة المستخرجة أم لا، ويستعان في ذلك بتكنولوجية الإعلام الآلي التي أثبتت دورها الفعال في تقديم التي تساهم في فهم مضمون وكينونة الدليل التقني، وكشف مدى التلاعب بمضمون هذا الدليل (الصغير، 2001).

2.1.استخدام عمليات حسابية خاصة تسمى بالخوارزميات: يتم اللجوء إلى هذه العملية عادة في حالة عدم الحصول على النسخة الأصلية للدليل الالكتروني أو في حالة ما إذا كان هناك شك في أن التغيير قد مس النسخة الأصلية، فهنا تسمح هذه التقنية بالتأكد من مصداقية الدليل وسلامته من التغيير.

2. تقييم الدليل الإلكتروني في السلامة الفنية لإجراءات تحصيله: إذا كانت نسبة الخطأ الفني في الحصول على الدليل الالكتروني ضئيلة جدا باعتباره تطبيقا من تطبيقات الدليل العلمي الدقيقة، فذلك لا يعني أنها منعدمة تماما، إنما يظل الوقوع في الخطأ ممكنا أثناء استخلاصه.

ج: وجوب مناقشة الدليل الإلكتروني:

إن تحقق شرط المشروعية وشرط سلامة الدليل الإلكتروني من التغيير وسلامته من الخطأ في إجراءات التحصيل، لا يكفي لاكتسابه قوة في الإثبات، بل لابد أيضا من مناقشة هذا الدليل بصفة علنية في جلسة المحاكمة وفقا لمبدأ أساسي في قانون المسطرة الجنائية هو مبدأ الشفوية والمواجهة، بمعنى أن القاضي لا يمكنه أن يؤسس اقتناعه إلا على العناصر الإثباتية التي طرحت في جلسات المحاكمة وخضعت لحرية مناقشة أطراف الدعوى (الصغير، 2001)، وهو ما أكدته محكمة النقض في أحد قراراتها بأنه:" بمقتضى المادة 287 من قانون المسطرة الجنائية، فإن القاضي لا يمكن له أن يبني مقرر إلا على حجج عرضت أثناء الإجراءات ونوقشت شفهيا وحضوريا أمامه، ولهذا يتعرض للنقض المقرر الذي بني على علم رئيس الجلسة عندما قام بالتحقيق في قضية سابقة" وعليه فإذا كان القاضي لا يمكنه أن يحكم استنادا إلى علمه الشخصي، فإن ذلك يحتم عليه أن تتم مناقشة كافة الأدلة المتولدة من الحواسب الالكترونية القائمة في ملف الدعوى لكي يتمكن من تكوين اقتناع يقربه نحو الحقيقة الواقعية التي يصبو إليها كل قاض عادل، فمثلا بالنسبة لشهود الجرائم الإلكترونية الذين تم سماعهم من قبل في التحقيق الإعدادي فإنه يجب إعادة سماعهم مرة أخرى أمام محكمة الموضوع، ونفس الأمر ينطبق على خبراء الأنظمة الإلكترونية على اختلاف تخصصاتهم ينبغي أن يمتثلوا أمام المحكمة لمناقشة تقاريرهم التي أعدوها.

وبهذا فإنه إذا كان القانون يشترط لاكتساب الدليل الالكتروني قوته الثبوتية أن يكون مشروع وأن يخضع لمناقشة علانية، فإن دور القاضي في ذلك يبقى محدودا جدا بسبب النقص الفادح في ثقافته الإلكترونية، وهو ما جعل البعض يقول بأن التطور العلمي من شأنه أن يطغى على نظام الاقتناع القضائي، ولا يبقى للقاضي إلا الاستعانة بالخبراء التقنيين المختصين دون أي تقدير من جانبه.

ثانيا: مبدأ الاقتناع القضائي في تقدير الأدلة الالكترونية.

يعد مبدأ الاقتناع القضائي أحد أهم المبادئ التي تقوم عليها نظرية الإثبات الحر، لأن القاضي لا يقيده المشرع بأدلة إثبات معينة وإنما يترك له حرية الإثبات وفقا لسلطته التقديرية في تقدير الدليل. وهذا ما أكده المشرع المغربي عندما نص في الفقرة الأولى من المادة 286 من قانون المسطرة الجنائية على أنه: " يمكن إثبات الجرائم بأية وسيلة من

وسائل الإثبات، ما عدا في الأحوال التي يقضي القانون فيها بخلاف ذلك، ويحكم القاضي حسب اقتناعه الصميم ويجب أن يتضمن المقرر ما يبرر اقتناع القاضي وفقا للبند 8 من المادة 365 الآتية بعده".

وأمام الارتفاع المتزايد للجرائم الالكترونية وتعاظم أساليب وتقنيات ارتكابها، أدى ذلك إلى انضمام الدليل الالكتروني إلى حقل الأدلة العلمية الجنائية الموثوقة واحتلاله مرتبة أفضل مما فرض على القاضي الجنائي التعامل معه رغم نقص ثقافته الإلكترونية من جهة، والقيمة العلمية التي يتمتع بها الدليل من جهة أخرى. ومام هاتين المعادلتين يثار التساؤل التالي، هل يبني القاضي الجنائي اقتناعه بالدليل الالكتروني على أساس أنه محسوم علميا؟ أم أن ذلك يدخل في محض تقديره الشخصي مثله مثل باقي الأدلة؟

انقسم الفقه في هذه المسألة إلى من يرى بأن الدليل الالكتروني بحكم أصالته العلمية ودقته الفنية التي يبلغ معها إلى درجة اليقين له قوته الثبوتية الملزمة للقاضي (جمال، التحقيق الجنائي في الجرائم الإلكترونية، 2018)، وحجتهم في ذلك أن الدليل العلمي هو النتيجة التي تسفر عنها التجارب العلمية لإثبات أو نفي الواقعة التي يثار الشك حولها، والتي غالبا ما يتطلب فهمها معرفة ودراية خاصة قد لا يملكها القاضي بحكم تكونه القانوني المحض.

ويخلص هذا التجاه إلى القول بأن الأدلة الالكترونية تتمتع بحجية قاطعة في الدلالة على الوقائع التي تتضمنها، ويمكن التغلب على مشكلة التشكيك في مصداقيتها من خلال إخضاعها لاختبارات تسمح بالتأكد من صحتها وسلامتها، ويجب عدم الخلط بين بين الشك الذي يشوب الدليل الالكتروني بسبب امكانية العبث به أو لوجود خطأ في الحصول عليه، والقيمة الاقناعية لهذا الدليل. ففي الحالة الأولى فإن القاضي لا يملك الفصل فيها لأنا مسألة فنية بحتة والقول فيها هو قول أهل الاختصاص، أما في الحالة الثانية فهي عندما يكون الدليل الالكتروني خالي من أي عبث، بمعنى أن تتوافر فيه الشروط المذكورة من قبل، فلن يكون للقاضي هنا إلا قبول هذا الدليل والاقتناع به، ولا يمكنه رده أو التشكيك في قيمته الثبوتية لكونه وبحكم طبيعته الفنية يمثل إخبارا صادقا عن الوقائع، ما لم يثبت عدم صلة هذا الدليل بالجريمة المراد إثباتها.

واسترشادا بذلك، يمكن القول بأن أصحاب هذا الاتجاه قد جعلوا الطبيعة العلمية للدليل الالكتروني قيدا حقيقيا لحرية القاضي الجنائي في تقدير الدليل يجبره على الاقتناع به والحكم بمقتضاه ولو لم يكن مقتنعا بصحة الواقعة المطروحة أمامه، إذ لم يعد القاضي وفقا لهذا الاتجاه حرا في مناقشة تقدير الدليل العلمي الذي أصبح يؤدي دور الصدارة في الإثبات الجنائي ف الجرائم الالكترونية.

وخلافا لما ذهب إليه الاتجاه الفقهي الأول، هناك من يرى بأن مبدأ حرية القاضي في الاقتناع يجب أن يبسط سلطانه على كل الأدلة دون استثناء بما فيها الدليل الالكتروني، معبرين بأن إعطاء الدليل الالكتروني قوة ثبوتية مطلقة لا يستطيع القاضي مناقشتها أو تقديرها يعد بمثابة رجوع إلى الوراء إلى نظام الإثبات المقيد (إسماعيل، 1992). كما يضيف هذا الاتجاه بأن توافر الدليل الالكتروني لا يعني التزام القاضي بالحكم بموجبه مباشرة بالإدانة أو بالبراءة، لأن الدليل الالكتروني ليس آلية معدة لتقرير القاضي بخصوص مسألة غير مؤكدة.

وحسب هذا الاتجاه، فإنه مهما يعلى شأن الأدلة الالكترونية في مسألة الإثبات الجنائي، فإنه يجب الإبقاء على سلطة القاضي في تقدير هذه الأدلة وتكوين قناعته بكل حرية، وذلك لأن القاضي يظل هو المسيطر، حيث من خلال سلطته التقديرية يستطيع أن يفسر الشك لصالح المتهم، ويستبعد الأدلة التي تم الحصول عليها بطرق غير مشروعة، ويجعل من الحقيقة العلمية حقيقة قضائية.

المحور الثاني: مظاهر صعوبات الاثبات في الجريمة الالكترونية.

يكتنف إثبات الجرائم الإلكترونية صعوبات جمة ترجع لأسباب عديدة أهمها عدم وجود أثر مادي للجريمة المرتكبة، كما أن الجاني يستطيع تدمير دليل الإدانة في أقل من ثانية، والأكثر من ذلك أن الإجرام المعلوماتي لا يعترف بالحدود إذ أن الجريمة قد تتم من مسافات بعيدة عبر اتصال هاتفي يمكن للجاني من خلاله إعطاء تعليماته للحاسب الآلي، ومما يزيد من استعصاء إثبات هذه الجرائم أن المجني عليهم يحجمون عن الإبلاغ عن وقوعهم ضحية لها، بل حتى في حالة استطاعة السلطات المعنية وضع يدها على البعض منها فإن الضحايا يمتنعون عن مساعدة هذه السلطات أملا في استقرار حركة التعامل ويفضلون إخفاء أسلوب ارتكاب الجريمة مخافة إتاحة الفرصة للآخرين لتقليدها، وبالتالي فإن الحصول على الدليل الإلكتروني واعتماده في إثبات الجرائم الإلكترونية تواجهه مجموعة من العراقيل الموضوعية (أولا)، والإجرائية (ثانيا).

أولا: المشكلات الموضوعية للدليل الإلكتروني.

ترجع هذه المشاكل إلى طبيعة الدليل ذاته نظرا للخصائص الفيزيائية التي يتكون منها هذا الدليل، سواء فيما يخص الطبيعة غير المرئية له، أو بسبب مشكلة الأصالة أو سبب ديناميكيته.

1- الدليل الإلكتروني دليل غير مرئي: فهو عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي، وبطريقة غير منظمة، فعلى سبيل المثال تتضمن الأقراص الصلبة مزيجا من بيانات مختلطة فيما بينها مما يؤدي إلى اختلاط الأمور فيما بينها بمعنى أنه قد تختلط الملفات البريئة مع تلك المجرمة التي تعد موضوعا للدليل الجنائي الرقمي مما يؤدي إلى خلق مشكلة التعدي على الخصوصية.

وبالتالي نستشف أن الدليل الرقمي يختلف عن الأدلة الناتجة عن الجرائم التقليدية من حيث الآثار المترتبة عنه (كالأسلحة النارية أو المادية، أو المحرر ذاته الذي تم تزويره)، مما يسهل على رجال العدالة الجنائية إثباتها، عكس الجرائم الإلكترونية حيث يكون ذلك في منتهى الصعوبة باعتبار أن الدليل الإلكتروني هو عبارة عن نبضات إلكترونية مكونة من سلسلة طويلة من الأصفار يصعب التعرف على جناتها، زيادة على ذلك غالبا ما يكون الدليل الرقمي مرموزا أو مشفرا، كما أنه يمكن التلاعب فيه وتعديله، مما يؤدي إلى إزالة السبب ما بين المجرم وجريمته ويحول دون كشف شخصيته، وبالتالي يشكل هذا الدليل نوعا مغايرا لما اعتاد على إثباته رجال الضابطة القضائية (عازف، 2019).

2 مشكلة الأصالة في الدليل الإلكتروني: إن قبول الدليل الإلكتروني كوسيلة للإثبات يطرح مجموعة من التساؤلات حول مصداقيته، ومن أهمها مشكلة الأصالة وبعبارة أخرى مشكلة الاعتداد بالنسخة، ذلك أن طبيعة الكتابة عبر

الحاسوب تجعل من المخرجات مجرد نسخ للأصل الموجودة رقميا في الحاسوب أو عبر الانترنت، فالدليل يعرض أمام القضاء في شكل مستندات مطبوعة أوكبيانات معروضة على شاشة الكمبيوتر مما يجعلها نسخا للأصول، أو دليلا ثانويا لا أصليا

الأصالة في الدليل الإلكتروني لها طابع افتراضي، لا يصل أو يرق إلى درجة الأصالة في الدليل المادي، حيث يعبر هذا الأخير عن وضعية مادية ملموسة، كما هو الشأن بالنسبة للمحررات المكتوبة أو بصمة الأصابع، في حين أن الدليل الرقمي المعبر عن التزييف الإلكتروني عبارة عن تعداد غير محدود لأرقام ثنائية موحدة في الصفر والواحد(0-1)، فالصورة مثلا التي توجد في العالم الرقمي ليس لها ذلك الوجود المادي الذي تعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فكل شيء في العالم الرقمي يتكون من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها وتفاعلها من الطاقة، ولقد أثارت مشكلة الأصالة جدلا على المستوى القانوني الأمر الذي جعل التشريعات المقارنة تفترض أصالة الدليل الإلكتروني (مختاري، 2014) .

وتطرح حجية الصور الورقية للدليل الإلكتروني مشكل مدة الانطباق أو التماثل بين الأصل الورقي الثابت ماديا وبين الدعامة الإلكترونية المتغيرة لاختلاف طبيعة كل منهما، ويزداد المشكل أمام سكوت المشرع عن تبيان قيمة الصورة المنسوخة على الورق من الدليل الإلكتروني، ومن ثم يستوجب الرجوع إلى القواعد العامة التي تعطي للصورة حجية الأصل بشرط أن تكون الصورة رسمية، وهذا ماتنبه له المشرع المغربي من خلال مشروع قانون المسطرة المدنية فيما يخص استعمال الوسائط الإلكترونية في المادة المدنية.

وهو الأمر الذي عمل به قانون الإجراءات الجنائية للولايات المتحدة الأمريكية من خلال نص صريح جاءت به القاعدة (1001 في بندها 3)، حيث سمح هذا القانون استثناء بقبول الدليل الإلكتروني باعتباره مستندا أصليا ما دام أن البيانات صادرة من كمبيوتر أو جهاز مماثل وسواء كانت هذه البيانات مطبوعة أم مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبر عن البيانات الأصلية بشكل دقيق، (مختاري، 2014) وبالتالي تتساوى الكتابة المادية من حيث الأصالة مع مخرجات الحاسوب رغم أن طبيعة الكتابة عبر الحاسوب تجعل من المخرجات مجرد نسخ للأصل الموجود رقميا في الحاسوب، مما يسمح بقبول مخرجات الحاسوب كدليل إلكتروني.

3- الدليل الإلكتروني ذو طبيعة ديناميكية : فهو ينتقل عبر شبكات الاتصال بسرعة فائقة، بمعنى إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد، ويترتب على ذلك صعوبة تعقب الأدلة الرقمية وضبطها، لأنه يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها، (Zakaras، 2016) مثل معاينة مواقع الانترنت المخالفة، تفتيش نظم الحاسب الآلي، أو ضبط الأقراص الصلبة التي تحتوي على مواد غير مشروعة كالصور الإباحية مثلا، مما يؤدي إلى الاصطدام بمشاكل الحدود والولايات القضائية، ويرجع السبب في ذلك إلى أن هذه الإجراءات تمثل مساسا بسيادة الدولة التي عبر من خلالها نشاط المجرم وهو في طريقه للهدف، أو حيث قد توجد أدلة الجريمة، وهو ما ترفضه الغالبية العظمى من الدول، لذلك أبرمت العديد من الاتفاقيات والمعاهدات

الدولية في مجال التعاون الدولي التي تستهدف من وراء ذلك التقريب بين القوانين الجنائية الوطنية من أجل جمع هذا النوع من الأدلة العابرة للحدود خاصة في إطار مكافحة الجرائم العالمية ومنها الجرائم الإلكترونية.

ثانيا: العراقيل الإجرائية.

بالإضافة للمشاكل التي تعود لطبيعة الدليل الإلكتروني فإن هناك مشاكل إجرائية ترتبط إما بارتفاع تكاليف الحصول عليه، أو بنقص الخبرة الفنية والتقنية لدى سلطات الشرطة القضائية والتحقيق والقضاء بمجال تقنية المعلومات، لذلك سنحاول بحث كل مشكلة على حدة.

وعليه يمكن رد هذه العراقيل إلى ما يلي:

1. ارتفاع تكاليف الحصول على الدليل الإلكتروني: غالبا ما تطرح الجرائم الفنية مشكلة اللجوء إلى الخبرة في مجال التعامل مع أي ظاهرة فنية كما في جريمة التزييف سواء التقليدي منها أو الإلكتروني، إلا أن هذه الخبرة تشكل إرثا أو عبئا ثقيلا على العدالة الجنائية (مختاري، 2014)، بالنظر إلى حجم وضخامة المصاريف التي يتم إنفاقها في الحصول على الدليل الرقمي، ويزداد المشكل أمام غياب منظمات متخصصة بالجامعات والمعاهد لاسيما في الدول العربية والمغرب على وجه الخصوص. .مما يتطلب معه الأمر اللجوء إلى شركات أو منظمات أجنبية في الخارج، مما يجعل التكاليف تخضع للسعر العالمي المقرر في اللوائح المالية لتلك المنظمات (عازف، 2019).

2. نقص المعرفة التقنية لدى رجال العدالة الجنائية: إن الطبيعة الخاصة للدليل في مجال التزييف الإلكتروني كمثال ينعكس على عمل الجهات المكلفة بالبحث والتحقيق والمحاكمة، وهي مهمة تحتاج إلى الدراية التامة بطبيعة هذا النوع من الجرائم على نحو يساعدهم على مواجهة المشاكل التي تتعلق بإثبات تلك الجرائم، وللتعرف على شخصية مرتكبها وكيفية ارتكابها مع الاستعانة بوسائل جديدة، فمن المعلوم أن جهات البحث والتحري بطرقها التقليدية تجمع عناصر الإثبات عن طريق التفتيش والضبط، أي الآثار المادية، ولكن في محيط الجريمة الحالية التي تعتمد على استخدام التكنولوجيا، لا تستطيع تلك الجهات تطبيق إجراءات الإثبات التقليدية على جرائم التزييف الإلكتروني خاصة ما يتعلق بالأشياء المعنوية كمحل للجريمة. حيث تجد نفسها عاجزة في التعامل مع هذه النوعية من الجرائم، بل إن المحقق نفسه قد يدمر الدليل بخطأ منه أو بإهمال. (حسن، 2014) مما يستدعي إدراك ضباط الشرطة القضائية وسلطتا الاتهام والمحاكمة وكذا هيئة الدفاع محتوى المعلومات وجزئياتها ليتسنى إبداء الرأي في شأنها .

وعليه فيجب على كل دولة أن تنشأ إدارة متخصصة بهذا النوع من الإجرام، وذلك لتلقي البلاغات وملاحقة وتعقب مرتكبيها، وتقديمهم للمحاكم (عازف، 2019)، بالإضافة إلى ضرورة تدريب وتأهيل كل من جهاز التحري والبحث والتحقيق وخلق فضاء متخصص في الجرائم التي ترتكب عبر تقنية المعلومات، وتدريبهم على معالجة هذا النوع من القضايا التي تحتاج إلى خبرات فنية عالية لملاءمة قبول هذا النوع من الأدلة وتقديرها وهذا يقتضي تنمية استعدادهم الخاص وتكوين مهارات فنية خاصة، تتناسب مع حجم المتغيرات والتطورات المتلاحقة في مجال جرائم التقنية، بالموازاة مع ذلك نناشد بضرورة تطوير أساليب البحث عن الأدلة وتقديمها لتواكب هذا التطورات.

وكخلاصة لما سبق هناك قصور كبير على مستوى النصوص الجنائية الموضوعية والإجرائية، بحيث أن هذه النصوص قد أصبحت قاصرة وعاجزة عن كفاية الحماية الفعالة للمصالح والقيم التي أفرزتها ثورة الاتصالات عن بعد، الأمر الذي يدعو للتساؤل عن كيفية تعامل المشرع المغربي مع الجريمة الإلكترونية من حيث التنظيم والتأطير، وسيتضح لنا ذلك من خلال نموذج المس بسرية أنظمة المعالجة الآلية للمعطيات كأحد تطبيقات الجريمة الإلكترونية بالتشريع المغربي.

خاتمة:

إزاء التطور التكنولوجي والمعلوماتي واستخدام وسائط الكترونية في معالجة البيانات، ظهرت للواقع العملي وسائط حديثة في إبرام التصرفات القانونية تختلف في طبيعتها عن الوسائل التي اعتاد الأشخاص استخدامها، ومع الدخول الفعلي لهذه الوسائط حيز إبرام التصرفات، ظهرت مصطلحات جديدة في المجال القانوني الأمر الذي ترتب عليه طرح تحديات جديدة على الصعيد القانوني تتمثل في عدم استيعاب القواعد الحالية لهذه المصطلحات المستحدثة، وانطلاقا من ذلك وجدت الحاجة إلى ضرورة تطوير هذه القواعد لكي تستوعب المصطلحات المستحدثة، حيث إن التكنولوجيا اليوم تفوقت في وضع حلول جدية لتسهيل وإبراز نجاعة الجهاز القضائي عبر الاعتماد على الوسائل الإلكترونية الحديثة، والانتقال من المساطر المادية إلى مرحلة التجسيد اللامادي للمعطيات والبيانات .

ولا يسعنا القول في ختام هذا البحث إلا أننا حاولنا أن نتناول مسالة خصوصية القوة الثبوتية للدليل الالكتروني، الذي يخضع كغيره من الأدلة لنفس القواعد المتعلقة بمشروعيته وحجية قبوله على مستوى نظام الاثبات وكذا سلطة القاضي في تقديره والاقتناع به كدليل في الإثبات، وذلك من خلال رصد أهم الإشكالات التي تتعلق بطبيعة الأدلة الخاصة بالمعاملات الالكترونية التي أفرزتها الثورة الإلكترونية، حيث أدت إلى ظهور معاملات جديدة ذات طبيعة خاصة لا من حيث صورها ولا من حيث وسائل إثباتها وكيفية تعامل القانون وأجهزة العدالة معها.

أولا: أهم النتائج المتوصل بها:

- ✓ الدليل الالكتروني، هو ذلك الوسيلة الرقمية الناتجة من تقنية المعلومات والتي يتم التنقيب عنها في العالم الافتراضي ومن شكليات الاتصال والأجهزة الالكترونية.
- ✓ أهمية الخبرة المتخصصة في المساعدة على الحصول على الدليل الالكتروني وتكوين القناعة القضائية.
- ✓ قصور القواعد العامة الإجرائية التقليدية فيما يخص طرق الحصول على الدليل الالكتروني.
- ✓ ان الدليل الرقمي مثله مثل باقي الأدلة في إثبات الجريمة، فهو يخضع للسلطة التقديرية للقاضي الجنائي أي يخضع لقناعة القاضي.
- ✓ الدليل الالكتروني لا يقتصر استخدامه فقط لإثبات الجريمة الإلكترونية وإنما يستخدم في إثبات الجرائم التقليدية.

ثانيا: أهم التوصيات المقترحة:

- ✓ تأهيل جهاز العدالة في مجال التقنيات الحديثة بما يسمح لهم بتكوين خبرة في كيفية التعامل مع الجرائم الالكترونية ووسائل إثباتها وما تتمتع به من خصوصيات.
- ✓ ضرورة وضع قواعد وآليات خاصة لحفظ المحررات الالكترونية، وذلك بإنشاء مرافق تعمل على القيام بهذه المهمة، على ان تنظم هذه الاليات مسؤولية هذه المرافق عن الاخلال بسرية هذه المحررات.
- ✓ ضرورة اشتراط حد أدنى من الخبرة والكفاءة الفنية والتقنية للترخيص لجهات التصديق الالكتروني، حماية للمستفيدين وتعاملاتهم الالكترونية من اختراق أو افشاء.
- ✓ عقد ندوات علمية تكنلوجية من أجل مواكبة كل تطور سواء القانوني أو التقني الخاص بالمعاملات الالكترونية، إضافة إلى تبادل الخبرات والتجارب بين دوي الاختصاص، وخصوصا الأشخاص والجهات المهتمة بهذا المجال في الدول المتقدمة للاستفادة من تجاربهم القانونية والقضائية.

قائمة المراجع:

1) ابراهيمي، جمال. (2018). التحقيق الجنائي في الجرائم الإلكترونية. تيزي وزو، كلية العلوم القانونية والسياسية، الجزائر

2) إسماعيل, م. ع. (1992). مبدأ حرية القاضي الجنائي في الإقناع. القاهرة: دار المنارة .

3) إكرام، مختاري. (2014). تأثير ثورة التكنلوجيا على وسائل الاثبات الجنائية. مجلة العلوم القانونية .

4) جمال, ا. (2018). التحقيق الجنائي في الجرائم الإلكترونية. تيزي وزو ، كلية العلوم القانونية ، الجزائر

5) جمال، ا. (2018). التحقيق الجنائي في الجرائم الإلكترونية. تيزي وزو :جامعة مولود معمري-تيزي وزو -كلية الحقوق والعلوم السياسية، الجزائر.

6) جميل، عبد الباقي الصغير. (2001). أدلة الاثبات الجنائي والتكنوجية الحديثة . القاهرة : دار النهضة العربية

7) سعيد، عبد اللطيف حسن. (2014). إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت (الإصدار الطبعة الأولى). الاسكندرية: دار النهضة العربية.

8) فاضل، زيدان محمد. (2006). سلطة القاضي الجنائي في تقدير الأدلة . عمان : دار الثقافة للنشر والتوزيع .

9) لحسن، عازف. (2019). ماهية الدليل الرقمي وحجيته في الاثبات الجنائي . المغرب: مجلة الدفاع .

10) مصطفى، مجدي هرجة. (1999). الاثبات في المواد الجنائية في ضوء أحكام محكمة النقض. الاسكندرية : دار المطبوعات الجامعية .

11) Zakaras, M. R. (2016). International Computer Crime. revue international de droit pénal, 3ème et 4ème trimestres.

حول تجريم المخدرات الرقمية: الواقع والتحديات

On Digital Drug Criminalization: Reality and Challenges

د.محمد جلول زعادي/جامعة البويرة/الجزائر

Dr. Mohamed djelloul Zaadi/ University of Bouira/Algeria

ملخص الدراسة:

يمثل مكافحة المخدرات أحد أهم التحديات التي حُمل أعضاء المجتمع الدولي لرفعها، أيا كانت درجة تطورها، باعتبار إنتشار هذه الظاهرة لا ينحصر أثاره على الفرد من خلال الأضرار الجسدية والنفسية التي يخلقها الإدمان على مثل هذه المواد، وإنما تمتد لتشمل المجتمع برمته، نظرا إلى أنها أحد الأسباب الرئيسية في تشتت النسيج الإجتماعي، وأحد العوامل الجوهرية التي تقف في وجه النمو الإقتصادي للدول. ولكونها كذلك عملت المجتمعات كافة على التصدي لها بمختلف الوسائل التشريعية والميدانية بشكل يستحيل في ضوئه فهم الصموت الذي ثبتت عليه هذه الأخيرة بخصوص ظاهرة المخدرات الإلكترونية التي لا تقل خطورة عن المخدرات الكلاسيكية.

الكلمات المفتاحية: المخدرات الرقمية، الجريمة الدولية، المؤسسات العلاجية، الإدمان، الإتفاقيات الدولية، القانون الجزائري.

Abstract:

The fight against drugs represents one of the most important challenges that members of the international community have been urged to raise, regardless of the degree of its development, given that the spread of this phenomenon is not limited to the individual through the physical and psychological damage caused by addiction to such substances, but extends to include the entire community, given that it is one of the the main reasons for the dispersal of the social fabric, and one of the fundamental factors that stand in the way of the economic growth of countries. As such, all societies worked to confront it by various legislative and field means in a way that it is impossible to understand the silence that the latter has proven regarding the phenomenon of electronic drugs, which is no less dangerous than classic drugs.

Keywords: Digital drugs, International crime, Therapeutic institutions, Addiction, International conventions, Algerian law.

مقدمة:

شهد العالم خلال السنوات الأخيرة قفزة نوعية في مجال وسائل الإتصال بعد دمقرطة إستعمال شبكة الأنترنت من قبل الأفراد، وهو الأمر الذي غيّر بشكل جذري نمط حياة الأفراد على كافة الأصعدة من أبسطها إلى أكثرها تعقيدا، بدءا بالتعليم، ومرورا بالصحة، ووصولا للبيع والشراء. لم تقتصر الفوائد المنجرة عن مثل هذا التطور على الأفراد، وإنما إمتدت لتشمل كذلك الدول في حد ذاتها، هذه الأخيرة التي إستغلت التسهيلات التقنية التي صاحبت هذه القفزة النوعية لتطوير الخدمات التي تقدمها للمواطن، بالإضافة إلى شكل المبادلات التي تقدم علها مع غيرها من الدول وحجمها، وعرّضها في نفس الوقت لأشكال جديدة من التحديات ذات الصلة بتطور السلوك الإجرامي، والذي لم يعد ينحصر بدوره في المظاهر الكلاسيكية التي يتجسد فيها عادة، وإنما إتخذت من شبكة الأنترنت منصة لتنظيم نشاطها،

والإشارة في هذا الصدد تكون إلى الكيانات الإجرامية التي تستند إلى هذا النوع من الوسائل بإستدراج الأفراد الذين تستغل معاناتهم في إطار الهجرة غير الشرعية، أو الإتجار بهم كعبيد. وما يقال عن المنظمات الإجرامية ينطبق كذلك على التنظيمات الإرهابية التي أصبحت اليوم تجند عناصرها عبر مواقع التواصل الإجتماعي، وتنفذ عملياتها الإرهابية من خلال هذه الوسائط الإفتراضية.

ومن أهم المظاهر التي تجسد فيها تطور السلوك الإجرامي ظهور أشكال جديدة من الجرائم التي ترتكب بواسطة الشبكة العنكبوتية؛ فإلى جانب القرصنة، وسرقة البيانات، والتجسس، أصبحت المواقع الإلكترونية منصة لترويج المخدرات وبيعها، بما في ذلك المخدرات الإلكترونية، والتي كشفت الدراسات القليلة التي أنجزت حولها بأنها لا تقل خطورة عن المخدرات التقليدية.

الإشكالية:

إنطلاقا مما سبق ذكره يمكن طرح الإشكالية التالية:

ما مدى كفاية المنظومة القانونية السارية المفعول في مجال مكافحة المخدرات للتصدي لظاهرة المخدرات الإلكترونية؟

أهمية الموضوع:

يمكن أن نستخلص أهمية الموضوع محل الدراسة من خلال مجموعة من العناصر، لعل أهمها:

- ✓ تمثل المخدرات بصفة عامة، والمخدرات الإلكترونية بصورة خاصة آفة من الآفات الخطيرة التي تحمل كافة المجتمعات على التصدي لها، نظرا لآثارها الوخيمة على الأفراد، وما يستتبع ذلك من مظاهر غير أخلاقية؛
- ✓ تمثل المخدرات الإلكترونية أحد الأشكال الجديدة التي تجسدت فيها المخدرات، والذي كان ظهورها وإنتشارها نتيجة للتقدم الإلكتروني المحرز في مجال وسائل الإتصال؛
- ✓ إشتراك المخدرات الإلكترونية والمخدرات التقليدية في العديد من الخصائص، ولا سيما في الآثار المنجرة عن تعاطي هذا النوع من المخدرات.

أهداف الدراسة:

تصبو الدراسة الراهنة لتحقيق جملة من الأهداف، لعل أهمها:

- ✓ التعريف بالمخدرات الإلكترونية بإعتبارها نوعا مستحدثا من البرامج التي تأثر على عقل متعاطيها، وذلك برسم معالمها، وتحديد خصائصها، وتحديد الآثار المنجرة عنها على صحة المتعاطي النفسية والجسدية؛
- ✓ الكشف عن موقف التشريعات الوطنية والدولية إتجاه مسألة المخدرات الإلكترونية؛
- ✓ تحليل مدى ملائمة النصوص القانونية السارية المفعول في مجال مكافحة المخدرات مع خصائص المخدرات الإلكترونية، وبشكل خاص فيما يتعلق بالتدابير الوقائية والعلاجية المتخذة لمكافحة المخدرات التقليدية.

تقسيم الدراسة:

تنقسم الدراسة الراهنة إلى مبحثين متكاملين، يتعلق الأول بالإطار المفاهيمي للمخدرات الرقمية، حيث يتم في سياقه تحديد أصول المخدرات الرقمية والتعاريف المنسوبة إليها على الصعيد الفقهي، وبالتبعية إستخراج الخصائص التي تميزها عن غيرها من البرامج والمخدرات التقليدية، أما في إطار المبحث الثاني فسنبين فيه موقف التشريعات الوطنية وأعضاء المجتمع الدولي فيما تبنوه من إتفاقيات دولية من مسألة المخدرات الإلكترونية.

المنهج المتبع:

تم الإعتماد في إعداد هذه الورقة البحثية على مجموعة من المناهج العلمية، لعل أهمها: **المنهج الوصفي** الذي يتلائم مع الشطر النظري للدراسة، سيما ما يتعلق بسرد مختلف التعاريف المنسوبة للمخدرات الإلكترونية، أو سرد خصائصها، أو حتى تعداد النصوص القانونية المتعلقة بتعريف المخدرات في القانون الوطني والدولي. كما تم الإعتماد على **المنهج التاريخي** فيما يخص نشأة المخدرات الإلكترونية وتحديد جذورها التاريخية. هذا، وتم الإعتماد على **المنهج التحليلي** عندما يتعلق الأمر بتحليل مدى مطابقة النصوص القانونية السارية المفعول على الصعيدين الدولي والمحلي مع خصوصية المخدرات الإلكترونية.

المبحث الأول: الإطار المفاهيمي للمخدرات الرقمية

يعاني أعضاء المجتمع الدولي برمته من مساوئ المخدرات التي شهدت إنتشارا واسعا خلال السنوات الأخيرة، حيث أثبتت مختلف الدراسات التي أنجزت حول هذا الموضوع بأن تعاطي هذا النوع من المواد يلحق أضرارا جسمية وعقلية لا يمكن إصلاحها. ونظرا لخطورة هذا النوع من الممارسات تباينت المقاربات المتبناة من قبل هذه الدولة أو تلك من أجل التصدي لهذه الآفة السلبية بين مفضل للتدابير الردعية من خلال فرض عقوبات صارمة على منتجي، ومروجي، ومتعاطي هذا النوع من المواد، وبين المفضل للتدابير التوفيقية من خلال شرعنة هذا النوع من المواد، وتأطير بيعها، وإستهلاكها من خلال سن نصوص قانونية.

ترد المخدرات الرقمية في منطقة رمادية على المستوى التشريعي؛ فلم تكن موضوع تجريم، ولم يتم الترخيص بها في أي موضع من المنظومة القانونية السارية المفعول في هذا المجال، وهو الأمر الذي يدفعنا لعرض مختلف المحاولات التي تم الإقدام عليها من أجل تحديد معالم هذا المفهوم **(المطلب الأول)**، وبالتالي تحديد الأشكال التي يتجسد فيها على أرض الواقع **(المطلب الثاني)**.

المطلب الأول: تعريف المخدرات الإلكترونية

لم يكن التطور التكنولوجي في أي حضارة من الحضارات التي تعاقبت في هذا العالم مرادفا في كافة الحالات للإزدهار والرقي، وإنما خضعت في كل مرة لتحويل لأهدافها من قبل مجموعة من الأفراد لخدمة مصالح غير أخلاقية، وهو ذات الأمر الذي تعرضت له تقنية الأنترنت؛ فمن الهدف السامي الذي سطرت له هذه التقنية في الأصل، أي تسهيل حياة الأفراد، وظفت من قبل البعض لتدمير حياتهم، وظهور التداوي عن طريق النقر بالأذنين لم يسلم من هذا المنطق

(الفرع الأول)، بما أثار نزاعا وخلافا بين المختصين في هذا المجال حول المعنى الذي يمكن أن ينسب للبرامج الإلكترونية التي تحتوي هذا النوع من المخدرات **(الفرع الثاني)**.

الفرع الأول: نشأة المخدرات الإلكترونية

كانت البرامج المستعملة في إطار ما يسمى بتعاطي المخدرات الإلكترونية موجهة في الأصل لعلاج المرضى الذين يعانون من القلق والإكتئاب الخفيف، حيث كان اللجوء لهذا النوع من العلاج كوسيلة بديلة للعلاج الكيماوي الذي كان يقدم لبعض المرضى النفسيين عندما لا تجدي الأدوية الكيماوية نفعا. وتجدر الإشارة في هذا الصدد إلى أن هذا النوع من التداوي كان ثمرة تجارب أجراها للمرة الأولى العالم الفيزيائي الألماني "دوف فيلهام هايمريش" سنة 1839، وأطلق عليها تسمية طريقة "النقر بالأذنين"، هذه الطريقة تقوم على بث صوتين مختلفين في أذني المريض وفي آن واحد، بما يؤدي إلى سماعه صوت ثالث من شأنه التخفيف من الآلام النفسية للمريض (Ali, Soha, Nagla, & Nehad Ahmed, April 2019, p. 39).

ولقد كان للباحثة النفسانية الأمريكية " كيمبرلي يونغ" الفضل في تسليط الضوء للمرة الأولى على الخطر الذي يمثله تعاطي مثل هذه المخدرات، وهو ما أصطلحت عليه بتسمية "الإدمان على الفضاء السيبراني"، وبيّنت بأن الشبكة العنكبوتية أصبحت تحتضن بدءا من التسعينات من القرن الماضي مواقع متخصصة ببيع برامج تتضمن موسيقى خاصة مقابل مبالغ مالية معينة، كان بعض الأفراد يستمعون إليها من أجل التخفيف من حالتهم النفسية المتدهورة، وكان لجوئهم لهذا السلوك بعد أن إقتنعو بفعالية هذه البرامج من خلال الترويج لها عبر مواقع التواصل الإجتماعي (Fawzi & Farah A., 2017, p. 407).

الفرع الثاني: معنى المخدرات الإلكترونية

تجدر الإشارة باداء ذي بدء إلى أن المخدرات الإلكترونية لم تحض بالدراسة الكافية نظرا لحصرها في مجال العلوم الإجتماعية، وبالتحديد في مجال علم النفس، وهو ما يفسر غياب أي إشارة إليها في البحوث والدراسات القانونية، حيث إختلفت وجهات النظر حول طبيعة البرامج المتضمنة للمخدرات الإلكترونية؛ فمن الفقهاء من يركز على الوسائل المستعملة في عملية التعاطي، وبالتالي التخدير، ومنه من ركز على الآثار التي ينتجها تعاطي المخدرات الإلكترونية، في حين يبرز موقف وسط يمزج بين التوجهين بدمج المتغيرين. أدى الأمر الواقع إلى تضاعف المبادرات على الصعيد الفقهي من أجل تحديد معالم هذا المفهوم، لعل أبرزها التعريف الذي قدمه كل من الأستاذين "أميتال و ميهال" اللذان يريان بأن المخدرات الإلكترونية هي: "عبارة عن سلسلة من الملفات الصوتية، يتم الإستماع لها على نحو معين من خلال الإعتماد على سماعات الأذن، وتؤدي إلى إحداث أثار الهلوسة، أو تعديل الحالات المزاجية، والعاطفية، والبيولوجية لدى من يستمع لها، وتعديل قدرات الفرد على التركيز والتأمل والإنتباه، وتعتمد هذه الملفات الصوتية على عمل تزامن بين الصوت وموجات دماغية معينة، وتكون النتائج النهائية بعد سماع هذه الملفات دخول الفرد في حالة تتشابه مع الحالات التي يحدثها تعاطي المخدرات الواقعية مثل الماريخونة، أو الأفيون، أو الحشيش" (Amital & Mihal, 2011, p. 15)، كما يعرفها الأستاذ سعيد رفيق البربري بأنها: "مجموعة من المؤثرات الرقمية التي تعرض لها الخلايا العصبية

للإنسان عن طريق ملفات صوتية غير متزنة في آن واحد" (البربري، اكتوبر 2018، صفحة 11)، أما "توني كومفورد و فالنتينا لشتنر" يعرفانها بأنها: "ملفات صوتية يمكن تنزيلها والإستماع إليها من جهاز الكومبيوتر من خلال سماعات بجودة عالية، بحيث تصدر موسيقى المخدرات موجات كهرومغناطسية تؤثر على المخ من خلال تشجيع خلاياه العصبية على فرز هرمون السعادة، وبالتبعية تحسين مزاجه وزيادة سعادته"(Comford & Valentina, December 2014, p. 7) .

المطلب الثاني: أشكال المخدرات الإلكترونية وخصائصها

تمثل المخدرات الإلكترونية أحد الأشكال الجديدة التي تتجسد فيها المخدرات، غير أنها تتميز عن غيرها من الأشكال الأخرى في سهولة الوصول إليها بإعتبارها متوفرة على شبكة الأنترنت، كما أن تعاطيها يتم بسبل أخرى غير الحقن مثلا **(الفرع الثاني)**، غير أنها تشترك مع المخدرات التقليدية في نقاط أخرى مثل الآثار التي تنجر عنها، بالإضافة إلى إنقسامها إلى أنواع تتباين في مفعولها تبعا للأثر والإحساس الذي يصبو المتعاطي الوصول إليه من تعاطيها **(الفرع الأول)**.

الفرع الأول: الأشكال

لا تتجسد المخدرات الإلكترونية في برنامج واحد فحسب، وإنما تتضمن أنواعا مختلفة باختلاف الأثر الذي يريد المتعاطي أن يتعرض له؛ إذ يبين المختصون في هذا المجال بأن المخدرات الإلكترونية معروضة للبيع في المواقع المتخصصة في شكل أصناف وخفقات صوتية يحدد طبيعتها المشتري عند الطلب، ويتراوح ثمنها بحسب المفعول المرجو، ويبين هؤلاء بأن المخدرات الإلكترونية تحمل أسماء مختلفة تماثل تلك التي تحملها المخدرات التقليدية، فنجد مثلا المخدر المرسوم (**Sleeping Angle**)أو (**Delta**)، والذي يفترض فيه بأنه مساعد على النوم، أو مخدر(**Lucid Dream**)الذي يفترض بأنه يساعد المتعاطي على التخلص من الشعور بالآلام، كما نجد مخدرات تساعد الفرد المتعاطي على الهلوسة مثل مخدر (**Hands of God**)، والذي يفترض أن يحدث تخيلات وإلهام عند المتعاطي، ويمثل هذا الأخير من بين الأنواع الأكثر غلاء على الإطلاق. كما يدعي بعض المروجين أنه بإستطاعتهم إعداد برامج صوتية من شأنه مساعدة المتعاطي على إنقاص الوزن، أو حتى التخلص من الإدمان على التدخين (خلف، 2018، صفحة 25)

الفرع الثاني: الخصائص

تتميز المخدرات الإلكترونية عن غيرها من المخدرات التقليدية من خلال العناصر التالية:

أولا-موجات صوتية:

حيث تتجسد في ملفات صوتية خاصة تحتوي نغمات ذات تردد مختلف في الأذن اليمنى واليسرى، يستعمل في إطارها المدمن المتعاطي لهذا النوع من المخدرات سماعات ذات جودة عالية، بالإضافة إلى جهاز كومبيوتر أو هاتف نقال ذكي، ويقوم المتعاطي لهذا النوع من المخدرات بالإستماع لهذا النوع من الملفات في مكان هادئ، ومظلم، ومن هذه الخاصية تنجر خطورة هذه الممارسة، بإعتبار أن الكشف عن متعاطيها يعتبر أمرا شبه مستحيل (Comford &

Valentina, December 2014, p. 7).

ثانيا-تحميلها عبر شبكة الأنترنت:

من أهم مميزات المخدرات الإلكترونية أن يتم تحميلها عبر الشبكة الإلكترونية من مواقع متخصصة مثل موقع (I_DOSER) و(digipill)، والذي يكون في غالب الأحيان بمقابل مالي، وذلك في إطار شرعي كامل، من دون أي مراقبة، والملاحظ في هذا الصدد بأنه، وعلى خلاف المخدرات التقليدية فإن وصول الأفراد، بما في ذلك صغار السن لهذا النوع من البرامج سهل للغاية(abdulaziz, Eman, & khalil, 3-5 march 2019, p. 1) .

ثالثا-تحدث آثارا مماثلة للمخدرات التقليدية:

أثبتت الدراسات النادرة التي أنجزت حول موضوع تأثير المخدرات الإلكترونية أن تعريض الدماغ للنغمات الصوتية المتباينة التردد في الأذنين يؤدي إلى إفراز الدماغ هرمون السعادة، ويشعر الفرد بالسعادة والراحة، والإحساس بالألم، وهي آثار مماثلة لتلك المنجرة عن تعاطي المخدرات التقليدية مثل الحشيش، الهروين، والكوكايين (Jalal, abdelrazak, & Adil, 2020, p. 83).

المبحث الثاني: إستبعاد المخدرات الإلكترونية من دائرة التجريم

عمل أعضاء المجتمع الدولي جاهدين لمكافحة ظاهرة المخدرات التي ألحقت بمجتمعاتهم وإقتصادياتهم أضرارا بالغة الخطورة، بعد أن تمكن بارونات الإجرام عبر العالم من إيجاد السبل الكفيلة لإدخال سمومهم في مختلف الدول، واعتمدوا في ذلك بالدرجة الأولى على الفساد الذي يكمن في نفوس المسؤولين القائمين على شؤون أي دولة.

حمل الأمر الواقع السلطات العامة في كافة الدول على إتخاذ تدابير راديكالية للتصدي لهذه الظاهرة، سواء على الصعيد التشريعي من خلال ما تم سنه من نصوص قانونية على الصعيد الدولي **(المطلب الأول)**، أو على المستوى المحلي **(المطلب الثاني)**، أو من خلال التدابير الميدانية المتعلقة أساسا بمراقبة الحدود. وعلى الرغم مما أحرزته هذه التدابير من نتائج إيجابية، إلا أنها تبقى محدودة وعديمة النفع في مواجهة الصور الجديدة للمخدرات، كما هو الحال بالنسبة للمخدرات الإلكترونية التي لا تعتمد على ذات الطرق المعتمد عليها في إطار المخدرات التقليدية من حيث إنتاجها، أو توزيعها، أو حتى تعاطيها.

المطلب الأول: على الصعيد الدولي

تمثل الترسانة القانونية المتبناة على الصعيد الدولي حجر الأساس للمقاربة التي ثبت عليها أعضاء المجتمع الدولي لمكافحة المخدرات، بحيث تم تضمينها الجداول التي تحتوي على مختلف أصناف المخدرات الواقعة تحت طائلة التجريم. وعلى الرغم من التقدم والتطور الذي تنطوي عليه هذه الخطوة، إلا أن جمودها، وعدم مواكبتها للتطورات التي شهدها مجال الترويج للمخدرات وتوزيعها خلال السنوات الأخيرة جعل منها مجرد حبر على ورق عاجز على رفع التحديات التي تمثلها المخدرات المستحدثة مثل المخدرات الإلكترونية، هذه الأخيرة التي تتميز بتجاهلها من قبل السلطات العمومية،

سواء على الصعيد الدولي **(الفرع الأول)**، أو الإقليمي **(الفرع الثاني)**.

الفرع الأول: في الإتفاقيات الدولية

حضي موضوع مكافحة المخدرات بإهتمام أعضاء المجتمع الدولي منذ القدم، حيث توالت المبادرات الدولية لوضع حد لهذه الظاهرة التي لم تصبح مقتصرة في حدود دولة معينة، وإنما أصبحت تشمل العالم بأسره بعد أن إتخذت التنظيمات الإجرامية من الإتجار بهذه المواد مصدرا أساسيا لتمويل أنشطتها غير القانونية. ومن أهم الخطوات المقدم عليها في هذا الجانب تبني الإتفاقية الوحيدة للمخدرات لسنة 1961 (الإتفاقية الوحيدة للمخدرات بصيغتها المعدلة ببروتوكول ، 1972) التي تضمنت جداول مفصلة عن أنواع المخدرات الواقعة في دائرة اللاشرعية، غير أنها عرفتها بأنها: "كل مادة طبيعية أو تركيبية من المواد المدرجة في الجدولين الأول والثاني" (الإتفاقية الوحيدة للمخدرات بصيغتها المعدلة ببروتوكول ، 1972، الصفحات المادة الأولى فقرة 1- (ب))، كما تعرضت الدول المشاركة في إعداد إتفاقية المؤثرات العقلية لسنة 1971 لمسألة تعريف المؤثرات العقلية، وحصرتها في: "كل المواد سواء كانت طبيعية أو تركيبية. وكل المنتجات الطبيعية المدرجة في الجداول الأول أو الثاني أو الثالث أو الربع"، بينما حصرت المستحضر في: "كل محلول أو مزيج مهما كانت هيئته الطبيعية ويحتوي على مادة أو أكثر من المؤثرات العقلية.

2-كل مادة أو أكثر من المؤثرات العقلية يكون في شكل جرعات" (إتفاقية المؤثرات العقلية، 1971، صفحة المادة الأولى الفقرة (هـ) و (و)). هذا، ولا يسمح الرجوع إلى إتفاقية الأمم المتحدة الخاصة بالإتجار الغير المشروع للمخدرات والمؤثرات العقلية بتوضيح صورة المخدرات بشكل جلي، حيث ورد في الفقرة (ن) من المادة الأولى منها بأنه: "يقصد بتعبير المخدر أي مادة طبيعية كانت أو إصطناعية من المواد المدرجة في الجدول الأول والجدول الثاني من الإتفاقية الوحيدة للمخدرات سنة 1961..." (المتحدة، 1988، صفحة المادة الأولى الفقرة (ن)).

وبالرجوع إلى الجداول المشار إليها في الإتفاقيات الدولية نجدها تستبعد المخدرات الإلكترونية بصورة مطلقة، فإتفاقية المؤثرات العقلية لسنة 1971 تدرج في الجدول الأول المخدرات التي تطرح مخاطر سوء إستعمال عالية وتفرض تهديدا خطيرا على الصحة العامة وذات قيمة علاجية محدودة أو معدومة مثل حمض اليسرجيك إيفي لاميد، أما الجدول الثاني فيشار في إطاره إلى المخدرات التي تطرح مخاطر سوء إستعمال عالية وتفرض تهديدا خطيرا على الصحة العامة، وذات قيمة علاجية متوسطة أو منخفضة مثل الأمفيتامينات، أما الجدول الثالث فيشار فيه إلى المخدرات التي تطرح مخاطر سوء إستعمال، وتفرض تهديدا خطيرا على الصحة العامة، وذات قيمة علاجية متوسطة أو عالية، مثل الباربيتورات، في حين أن الجدول الرابع يشير إلى المخدرات التي تطرح مخاطر سوء إستعمال، وتفرض تهديدا بسيطا على الصحة العامة، وذات قيمة علاجية عالية مثل المهدءات.

أما فيما يخص المؤثرات العقلية، فيمكن أن نميز بين جدولين في إطار إتفاقية مكافحة الإتجار غير المشروع في المخدرات والمؤثرات العقلية لسنة 1988؛ ففي الجدول الأول يمكن أن نلاحظ سلائف المؤثرات العقلية مثل الإيفدرين، أما في الجدول الثاني يمكن أن نلاحظ مجموعة واسعة من الكواشف والمذيبات التي يمكن أن تستخدم في الإنتاج غير

المشروع للمخدرات والمؤثرات العقلية، والتي لها إستخدامات إصطناعية مشروعة وواسعة مثل الأسيتون) المخدرات, p. 9).

الفرع الثاني: في الإتفاقيات الإقليمية

تحذو الإتفاقيات الإقليمة حذو الإتفاقيات الدولية، سواء على الصعيد المفاهيمي، أو فيما يخص تصنيف المخدرات، ويضرب في هذا الصدد بالإتفاقية العربية لمكافحة الإتجار غير المشروع للمخدرات والمؤثرات العقلية لسنة 1946 (الإتفاقية العربية لمكافحة الإتجار غير المشروع للمخدرات و المؤثرات العقلية، 1946) مثالا عن ذلك، حيث عرفت في المادة 17 فقرة 1 المخدر بأنه: "أي مادة طبيعية كانت أو مصطنعة من المواد المدرجة في القسم الأول من الجدول الموحد"، وبالرجوع إلى الجدول الموحد المفصل في المادة 7 فقرة 1 منه نجدها تقضي بأن: "الجدول العربي الموحد للمخدرات والمؤثرات العقلية والمأخوذة عن إتفاقية الأمم المتحدة وتعديلاتها". يلاحظ ذات الموقف في سياق القرار الإطار المنبثق عن المجلس الأوروبي الصادر بتاريخ 25 أكتوبر 2004، والمتعلق بتأسيس الحد الأدنى للتدابير الخاصة بالعناصر المكونة للجرائم الجنائية والعقوبات الواجبة التطبيق في مجال الإتجار بالمخدرات، والذي تحيل المادة الأولى منه مسألة تعريف المخدرات إلى كل من الإتفاقية الموحدة للمخدرات لسنة 1961، واتفاقية المؤثرات العقلية لسنة 1971، وتنفي بالتالي إمكانية إدراج المخدرات الإلكترونية ضمن المخدرات المجرمة (europeene, 2004, p. article premier).

المطلب الثاني: على الصعيد المحلي

شارك عدد كبير من الدول في مختلف الإتفاقيات والمعاهدات الدولية التي تم سنها من أجل مكافحة ظاهرة المخدرات على يقين منها بأن التحدي الذي يمثله لا يمكن للدول منفردة أن تتحمله، وبالتالي فإن التعاون الدولي شكّل في نظرهم أفضل وسيلة للتصدي لهذه الظاهرة بالنظر إلى البعد العالمي الذي إكتسته هذه الأخيرة في الوقت الراهن. يلاحظ في هذا الصدد بأن التشريعات الوطنية لم تكن إلا إنعكاسا لما تم الإتفاق عليه على الصعيد الدولي في مجال مكافحة المخدرات بشكل ما يمكن ملاحظته في التشريع الجزائري **(الفرع الأول)**، أو في بعض النماذج المقارنة التي أخذنا منها عيّنات لإنجاز الدراسة الراهنة **(الفرع الثاني)**.

الفرع الأول: في التشريع الجزائري

لم يتعرض المشرع الجزائري هو الآخر لمسألة المخدرات الإلكترونية، بل وتميز موقفه فيما يخص تعريف المخدرات بصورة عامة بالغموض؛ بالرجوع إلى القانون رقم 04-18 المتعلق بالوقاية من المخدرات والمؤثرات العقلية وقمع الإستعمال والإتجار غير المشروعين بها الصادر بتاريخ 25 ديسمبر سنة 2004 نجده يعرف المخدر بأنه: "...كل مادة طبيعية كانت أو إصطناعية من المواد الواردة في الجدولين الأول والثاني من الإتفاقية الوحيدة للمخدرات لسنة 1961 بصيغتها المعدلة بموجب بروتوكل 1972" (قانون رقم 04-18 يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، 2004، صفحة المادة 2 فقرة 1)، أما المؤثرات العقلية فيعرفها بأنها:" كل مادة، طبيعية كانت أو إصطناعية، أو كل منتوج طبيعي مدرج في الجدول الأول أو الثاني أو الثالث أو الرابع من إتفاقية المؤثرات العقلية

لسنة 1971" (قانون رقم 04-18 يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، 2004، صفحة المادة 2 فقرة 2)، وبالرجوع لهذه التعاريف نجد بأن المشرع الجزائري يستبعد "البرامج"، مما يمكن أن يندرج تحت مظلة المخدر، بل وأكثر من ذلك، فإنه يربط المخدرات بعنصر مادي ملموس فمثلا يبين بأن المخدرات يتم إنتاجها، أي "عملية تتمثل في فصل الأفيون وأوراق الكوكا والقنب وراتينج القنب عن نباتاتها" (قانون رقم 04-18 يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، 2004، صفحة المادة 2 فقرة 13)، في حين أن المخدرات الإلكترونية يتم برمجتها بواسطة تطبيقات إلكترونية، كما يبين المشرع الجزائري بأن المخدرات يتم صنعها كذلك، أي "جميع العمليات، غير الإنتاج، التي يتم الحصول بها على المخدرات والمؤثرات العقلية، وتشمل التنقية وتحويل المخدرات إلى مخدرات أخرى" (قانون رقم 04-18 يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، 2004، صفحة المادة 2 فقرة 14)، في حين أن المخدرات الإلكترونية لا تخضع لمثل هذه العمليات. يبين المشرع الجزائري أخيرا بأن المخدرات يتم تصديرها وإستيرادها من دولة إلى أخرى، ويمكن في ذلك أن تتنقل عبر دولة عبور (قانون رقم 04-18 يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها، 2004، صفحة المادة 2 فقرة 15)، غير أن المخدرات الإلكترونية يتم تحميلها فقط عبر مواقع إلكترونية على شبكة الأنترنت.

هذا ولا تتفق التدابير الوقائية والعلاجية التي تبناها المشرع الجزائري لمعالجة الإدمان على المخدرات التقليدية مع خصوصية المخدرات الإلكترونية، فبالرجوع إلى المادة 6 من القانون 04-18 المشار إليه أعلاه التي يقضي فيها بأنه: "لا تمارس الدعوى العمومية ضد الأشخاص الذين إمتثلوا إلى العلاج الطبي الذي وصف لهم لإزالة التسمم واتبعوه حتى نهايته..."، على أن يتم هذا العلاج في إطار مؤسسة علاجية بشكل ما تفيد به المادة 22 من قانون العقوبات الجزائري (قانون رقم 16-02 يتمم الأمر رقم 66-156 المتضمن قانون العقوبات، 2016) الذي جاء فيها ما يلي: "الوضع القضائي في مؤسسة علاجية هو وضع شخص مصاب بإدمان إعتيادي ناتج عن تعاطي مواد كحولية أو مخدرات أو مؤثرات عقلية، تحت الملاحظة في مؤسسة مهيئة لهذا الغرض، وذلك بناء على أمر أو حكم أو قرار قضائي صادر من الجهة المحال إليها الشخص..."، هذه المؤسسات العلاجية لا تتطابق مع طبيعة الإدمان الذي يخلقه تعاطي المخدرات الإلكترونية، والذي يكون علاجه على المستوى النفسي أكثر منه على المستوى الكيماوي.

الفرع الثاني: في بعض الأنظمة المقارنة

نظرا للآثار الوخيمة المنجرة عن انتشار المخدرات في كافة المجتمعات لم يكن غريبا أن تحض مسألة مكافحتها بإهتمام أعضاء المجتمع الدولي، الذين أصدرت سلطاتهم تشريعات خاصة بمكافحة المخدرات، والملاحظ في هذا الصدد بأن المواقف قد تباينت حول المعنى المنسوب للمخدرات من دولة إلى أخرى، إلا أنها تتفق كلها حول الطبيعة المادية للمخدرات، فنجد مثلا المشرع البريطاني يعرف المؤثرات العقلية في قانون المؤثرات العقلية لسنة 2016 بأن المؤثرات العقلية هي: "(1) في مفهوم هذا القانون تعني المؤثرات العقلية (أ) مواد يمكن أن تحدث آثارا على عقل الشخص الذي يتعاطاها (...)

(2) يقصد في هذا القانون بالمواد التي تحدث آثارا على عقل المتعاطي كل المواد التي تنشط أو بالعكس تخلق حالة إنهيار في النظام العصبي للشخص الذي يتعاطاها، فهي تأثر على حالته النفسية بصورة عامة" (psychoactive substances act, 2016, p. article 2 para 1 and 2).

أما بالنسبة للدول العربية فالأمثلة كثيرة، ومنها نشير للمشرع الأردني الذي عرف هو الآخر المادة المخدرة في قانون المخدرات والمؤثرات العقلية لسنة 2016 (القانون الأردني الخاص بالمخدرات و المؤثرات العقلية، 2016)، والذي جاء في المادة 2 فقرة 2 منه ما يلي: "...كل مادة طبيعية أو تركيبية من المواد المدرجة في الجداول مواد الأرقام (1) و(4) الملحقة بهذا القانون"، بينما يعرف المؤثرات العقلية في المادة 2 فقرة 4 من ذات القانون بأنها: "... كل مادة طبيعية أو تركيبية من المواد المدرجة في الجداول ذوات الأرقام (5) و(6) و(7) و(8) الملحقة بهذا القانون"، أما المستحضر، فيقصد به: "...كل مزيج سائل أو جامد يحتوي على محضر وفقا لما هو منصوص عليه في الجدول رقم (3) الملحق بهذا القانون".

خاتمة:

يظهر من خلال ما سبق بأن التحدي الذي سترفعه الدول بعد تجريم محتمل للمخدرات الإلكترونية سيكون أكبر مقارنة بالمجهودات الحالية التي تبذلها من أجل التصدي للمخدرات التقليدية. وبالفعل، فإن سكوت أعضاء المجتمع الدولي، وتجاهلهم لهذه الظاهرة من شأنه أن يساعد في إنتشارها وتغلغلها في أعماق المجتمعات، بل وأكثر من ذلك باستهدافها لفئة الشباب وسهولة وصولهم إليها، فإن ذلك سينتج جيلا متأثرا بدرجات متفاوتة بهذه الظاهرة، خاصة وأن طرق التعافي منها شبه منعدمة. يفسر الأمر الواقع تضاعف الجهود المبذولة، سيما على الصعيد الفقهي الذي عمل أبرز ممثليه من خلال البحوث والدراسات الميدانية المنجزة رسم معالم هذه الظاهرة، وتحديد أثارها على الأفراد الذين يتعاطونها، وبالتالي الكشف عن المخاطر التي تنطوي عليها.

وعلى الرغم من الجهود المبذولة فإن هذه الأعمال لم تجد صدى لها في أعلى مستويات الدول، حيث تبقى محل تجاهل من قبل كبار المسؤولين، وهو الأمر الذي يكشف بدوره عن الإنشقاق الفادح الذي يفصل الجهات الحاكمة عن الواقع الذي يعيشه المجتمع.

من خلال ما سبق أفضت الدراسة المنجزة عن مجموعة من النتائج، لعل أهمها:

المخدرات الإلكترونية متجسدة على أرض الواقع في برامج إلكترونية يمكن تحميلها من مواقع متخصصة، ويستلزم تعاطيها جهاز كمبيوتر أو هاتف نقال ذكي، بالإضافة إلى سماعات عالية الجودة، يؤدي تشغيلها إلى بث نغمات مختلفة التردد من الأذن اليمنى إلى الأذن اليسرى، يحاول الدماغ توحيدها كآلية غريزية تحدث هذه المتغيرات تفاعلا في دماغ المتعاطي يشعره بنشوة مماثلة لتعاطي المخدرات الكلاسيكية.

لا تقل المخدرات الإلكترونية خطورة عن المخدرات التقليدية، فهي تحدث آثارا مماثلة للحشيش أو الكوكايين أو المارخوانة، بحسب نوع البرنامج المحمل، كما أن تعاطيها يقترن بإدمان المتعاطي لهذا النوع من البرامج، والتي يصل إليها الأفراد بشكل أسهل بمجرد الولوج لشبكة الأنترنت؛

على خلاف المخدرات التقليدية تحض المخدرات الرقمية بتجاهل تام من قبل السلطات العمومية في كافة الدول، بما يسهل الوصول إليها، وييسر ترويجها، وبيعها، وتعاطيها.

إنطلاقا مما ذُكِرَ آنفا، يمكن الوقوف عند مجموعة من الفراغات التي كشفت عنها الدراسة الراهنة، والتي يمكن تلخيص أهمها فيما يلي:

✓ ضرورة تبني إتفاقية دولية تتناول موضوع المخدرات الرقمية بالدراسة في أدق ثناياه، بدء بتحديد معالمه حتى يمكن تمييزه عن غيره من البرامج الصوتية الأخرى، مرورا بآثاره، والتي يتم بنائها على دراسات علمية محكمة ومؤطرة، ووصولا إلى التدابير الواجب اتخاذها للتصدي لهذه الظاهرة، أكانت تدابير وقائية أم علاجية، أو حتى ردعية فيما يخص المتعاطي في حد ذاته أو المروج أو البائع؛

✓ ضرورة التوعية حول المخاطر التي ينطوي عليها تعاطي هذا النوع من البرامج من خلال حملات توعوية يتم تبنيها، سواء في إطار مواقع التواصل الإجتماعي أو عبر مؤتمرات وملتقيات تنظم لهذا المبتغى.

قائمة المراجع:

باللغة العربية:

1) الإتفاقية العربية لمكافحة الإتجار غير المشروع للمخدرات و المؤثرات العقلية. (1946).

2) إتفاقية المؤثرات العقلية. (1971).

3) الإتفاقية الوحيدة للمخدرات بصيغتها المعدلة ببروتوكول . (19

4) رفيق سعيد البربري. (اكتوبر 2018). أثر إختلاف مصدر الدعم الموزع النقال في رفع مستوى الوعي بمخاطر المخدرات الرقمية. تكنولوجيا التعليم: سلسلة دراسات و بحوث، 28(04).

5) غازي حنون خلف. (2018). المخدرات الرقمية (نمط مستحدث و قصور في المواجهة التشريعية). مجلة رسالة الحقوق، السنة العاشرة(3).

6) القانون الأردني الخاص بالمخدرات و المؤثرات العقلية. (2016).

7) قانون رقم 18-04 يتعلق بالوقاية من المخدرات و المؤثرات العقلية و قمع الإستعمال و الإتجار غير المشروعين بها. (26 ديسمبر، 2004). الجريدة الرسمية(83). الجزائر العاصمة، الجزائر.

8) قانون رقم 16-02 يتمم الأمر رقم 66-156 المتضمن قانون العقوبات. (22 يونيو، 2016). الجريدة الرسمية(37). الجزائر العاصمة.

9) المفوضية العالمية لسياسات المخدرات. (بلا تاريخ). تصنيف المؤثرات العقلية: عندما يتم تجاهل العلم. تم الاسترداد من http://www.globalcommissiondrugs.org

10) منظمة الأمم المتحدة. (1988). إتفاقية الأمم المتحدة لمكافحة الإتجار غير المشروع في المخدرات و المؤثرات العقلية.

باللغة الأجنبية

11) Amital, & Mihal. (2011). The impact of digital medecines on youth congnition. journal of university of Bucharest.

12) Asmaa Mohamed Ali ،Kamel Mesbah Soha ،Fathi Mohamed Elattar Nagla و ،Zohra Nehad Ahmed) .April 2019 .(effect of digital drugs educational program on nursing students knowledge and attitudes at benha university .international journal of nursing didacts.(4)9 ،

13) Comford, T., & Valentina, L. (December 2014). Digital drugs: an anatomy of new medecines. 5th working conference on information systems and organizations.

14) Ekhlas abdulaziz ،abduljabar Eman و ،alsif khalil 5-3) .march 2019 .(feature extraction of music digital drugs properties based on contourlet transformation .international conference on computing and information science and technology and their application.

15) Fawzi, M. M., & Farah A., M. (2017). awarness on digital drugs abuse and its applied prevention among healthcare in KSA. Arab Journal of forensic medecine, 01(06).

16) journal officiel de l'union europeene 11) .novembre, 2004 .(la decision cadre 2004/757/jai du conseil concernant l'établissement des dispositions minimales relatives aux éléments constitutifs des infractions pénales et des sanctions applicables dans le domaine de trafic de drogue du 25 octobre 2004.

17) psychoactive substances act) .(2016) .chapter2.(

18) Zakaria K. Jalal ،A. mohammed abdelrazak و ،H. Mohamed Adil .(2020) .detention and evaluation of effective digital communication of drug on human body .Cihan university erbil scientific journal, (01)04 ،

المسؤولية الجزائية عن جريمة النصب والاحتيـــال الإلكتروني في التشريع الجزائري

Criminal Liability for the Crime of Fraud and Electronic Fraud in Algerian Legislation

ط.د.محمـد فواتيح/جامعة سيدي بلعباس /الجزائر
PhD.Mohamed Fouatih/ University of Sidi Bel Abbes/ Algeria

ملخص الدراسة:

إنّ حداثة التكنولوجية وتبلورها سريع الالتهاب في شتىّ المجالات وخصوصاً في أسرة الوطنية أصبحت لها خطورة تمّس كيان البشري في أمنه وبلده، وتزعماً من الدولة الجزائرية قامت باستصدار مجموعة من قواعد وأحكام معاصرة تصدّياً للجرائم الإلكترونية ورتّبت تفنينات حديثة لهاته العولمة تضبط فيها مستخدمي الانترنت مع إقرار المسؤولية الجزائية تفادياً من الانحراف الإلكتروني وأشكاله.

الكلمات المفتاحية: النصب والاحتيال، الجريمة الالكترونية، الشبكة العنكبوتية، الهيئات التشريعية

Résumé:

La Nouveauté De La Technologie Et Sa Cristallisation Rapide Dans Divers Domaines, En Particulier Dans La Famille Nationale, Est Devenue Dangereuse Pour L'entité Humaine Dans Sa Sécurité Et Son Pays, Et Sous La Direction De L'état Algérien, Elle A Edicté Un Ensemble De Règles Et De Dispositions Contemporaines Pour Lutter Contre La Cybercriminalité Et A Aménagé Des Lois Modernes Pour Cette Mondialisation Qui Contrôlent Les Internautes Avec La Reconnaissance De La Responsabilité Pénale Pour Eviter La Déviation Electronique Et Ses Formes.

Mots Clés : escroquerie, cybercriminalité, Internet, Cybercriminalité, mécanismes législatif.

مقدمة:

اعتبر القرن العشرين قرن الاختراعات الهائلة على المستوى التقني بفضل ظهور وانتشار استعمال الكمبيوتر واستحداث شبكات المعلومات وتوغّل الدقيق المكثّف، حيث أصبحت المعلوماتية وأدواتها وسائل ضرورية في العمليات البنكية أو سجلات الشركات وحتى علاقات الدولة مع الأفراد، وعلى الرغم من أهمية الوسائل الالكترونية وإيجابيات واستعمالها؛ إلا أنّ الاستخدام غير المشروع لها، قد أدّى إلى ظهور نوع جديد من الجرائم سميت بـ : "الجرائم الالكترونية "أو" الجرائم المعلوماتية " أو "جرائم الانترنيت"، وهذه المصطلحات كلها تعبّر عن مجموعة الجرائم المرتبطة بالأنظمة الإلكترونية والشبكة المعلوماتية وخصوصاً على شبكة الانترنيت، حتى أصبح يعرف بـ : " قرن المعلوماتية ".

وعلى هذا الأساس وجب العمل على سن قوانين تقر الحماية الجنائية للمعلومات المدخلة والمرتبطة بالحواسيب. إذ أن الجرائم المعلوماتية فرضت على العالم ضرورة تكييف قوانينها للتعامل مع هذا النوع من الإجرام الذي بات يهدد امن المجتمعات، كونه يتميز بامتداده وأنه عابر للأوطان ولا يقتصر على مكان ارتكابه فقط، والجزائر بدورها ركزت على الجريمة المعلوماتية وحاولت وضع مجموعة من الآليات الموضوعية والإجرائية لمواجهة هذا النوع من الإجرام. .وعلى هذا الأساس يطرح الإشكال في هذا المجال هو : كيف تصدى المشرع الجزائري لجريمة النصب والاحتيال الالكتروني؟

وللإجابة على هذه الإشكـالية، تمّ تقسيم هذه الدراسة إلى محورين:

- **المحور الأوّل:** خصوصيات جريمة النصب والاحتيال الإلكتروني وفق التشريع الجزائري.
- **المحور الثاني:** مدى فعالية العقاب المقرّر لجريمة النصب والاحتيال الإلكتروني.

وسوف نتبع طريقة المنهج الاستقرائي بدراسة أهم النقاط التي نظمت جريمة النصب والاحتيال الالكتروني محل الدراسة الحالية بخصوص النتائج المرجوة من هذه الدراسة هو: معرفة دور التشريعات التي سنها المشرع في محاربة جريمة النصب والاحتيال الالكتروني، وهل أدت ما عليها أو يجب على المشرع تداركها والبحث في نماذج أخرى جديدة لمحاربة تفشي هذه الجريمة في البلاد وتحقيق حماية حقيقية المرجوة.

المحور الأوّل: خصوصيات جريمة النصب والاحتيال الإلكتروني وفق التشريع الجزائري.

إنّ بروز العولمة وانتشار الرهيب وتحرّك السريع في ارتكاب الجرائم المستحدثة بوجود الانترنت التي أفرزت نوعا جديدا يختلف عن الجرائم التقليدية، وساهم في توسعها الاستخدام الكبير للشبكة العنكبوتية، ونشوء مجتمع معلوماتي تسيطر فيه الأجهزة الإلكترونية على لأذهان مستخدميه، وخاصة مع الدراية الكافية بمختلف التقنيات والبيانات المخزنة، ويتسم هذا النوع من الجرائم بسهولة ارتكابها وسرعة انتشارها بين الدول والقارات، وتعد جريمة الاحتيال الإلكتروني إحدى أهم الجرائم الإلكترونية التي تعتمد على أسلوب الخداع والغش للاحتيال على مال الغير اعتماد على تقنية الشبكة المعلوماتية في البيانات والمعلومات الالكترونية. وعلى ضوء هذا المحور سوف نتطرق إلى تبيان مقصود الجريمة في المطلب الأوّل؛ وفي المطلب الثاني تقنيات وإمكانيات المستحدثة في ارتكاب جريمة النصب والاحتيال وفق تقنين الجزائري.

المطلب الأوّل: تعريف الجريمة الإلكترونية.

صدر أول نص تشريعي جزائري في مجال الإجرام المعلوماتي في: 26 جويلية 2001م بموجب القانون رقم: 01-09 في المواد 144 مكرر و146 و144 مكرر 1 و144 مكرر 2 و146 من قانون العقوبات الجزائري والمتعّلق بجريمة القذف والسب إزاء رئيس الجمهورية أو فيما يخص دين الإسلام، أو ضدّ الهيئات العمومية، (العمومي، 2012) حيث أدرج المشرع فيها لأول مرة مصطلح وسيلة الكترونية أو معلوماتية وبعدها جاء القانون رقم: 04- 15 المؤرخ في: 10 نوفمبر 2004م في الفصل السابع مكرر تحت عنوان: " المساس بأنظمة المعالجة الآلية للمعطيات " (بوضياف ، 2018، ص. 352)من المواد 394 مكرر إلى المواد 394 مكرر 7، (قانون العقوبات، 2004)ولقد تم تعديل هذا القانون بموجب القانون رقم: 09 – 04 المؤرخ في: 14 شعبان 1430ه الموافق لـ: 05 أوت 2009م والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها (نمديلي ، 2022).

وللجريمة عدّة مسمّيات؛ فمنهم من ينعتها بـ: " جرائم الحاسوب " أو «الانترنيت "، أو «جرائم التقنية العالية " أو «جرائم الياقات البيضاء "، ومع تعدد المسميات تتعّدد التعاريف فمنهم من يعرّفها من جانب فني (تقني)، أما التعاريف الأخرى فيطغى عليها الجانب القانوني.

فمنهم من يعرّف الجريمة المعلوماتية على أنّها: " فعل ضار يستخدم الفاعل، الذي يفترض أن لديه معرفة بتقنية الحاسوب، نظاماً حاسوبياً أو شبكةً حاسوبيةً للوصول إلى البيانات والبرامج بغية نسخها أو تغييرها أو حذفها أو تزويرها أو تخريبها أو جعلها غير صالحة أو حيازتها أو توزيعها بصورة غير مشروعة " (حفوظة، 2022).

ويعرّفها " أحمد صياني " بأنّها: «تصرّف غير مشروع يؤثر في الأجهزة والمعلومات الموجودة عليها، وهذا التعريف يعتبر جامع مانع من الناحية الفنية للجريمة الإلكترونية، حيث أنّه لارتكاب الجريمة يتطلب وجود أجهزة كمبيوتر زيادة على ربطها بشبكة معلوماتية ضخمة". (حفوظة، 2022)

والبعض الآخر يعرّفها بأنّها: " الجرائم التي ترتكب ضدّ أفراد أو مجموعات مع وجود دافع إجرامي لإلحاق الضرر عمدا بسمعة الضحية، أو التسبّب بالأذى الجسدي أو النفسي للضحية بشكل مباشر أو غير مباشر، باستخدام شبكات الاتصال الحديثة مثل: الإنترنت (غرف الدردشة، البريد الإلكتروني..)، والهواتف الجوالة (الرسائل النصية القصيرة ورسائل الوسائط المتعددة)، وتشمل الجرائم الإلكترونية أي فعل إجرامي يتم من خلال الحواسيب أو الشبكات كعمليات الاختراق والقرصنة، كما تضم أيضا أشكال الجرائم التقليدية التي يتم تنفيذها عبر الإنترنت.(حفوظة ، 2022)

لقد اختلف بعض الدارسين والفقهاء في المجال القانوني؛ شريطة الغوص في عرض تعاريف الجريمة الالكترونية، لابد من الإشارة إلى المصطلحات المتعلقة بهذه الجريمة والتي نذكر منها:

أ. **التعريف الجريمة الإلكترونية بمفهوم الضيّق:**

ويرى الأستاذ {MASS} أنّ المقصود بالجريمة المعلوماتية: "الاعتداءات القانونية التي ترتكب بواسطة المعلوماتية بغرض تحقيق الربح".

كما أن مجرد استخدام الحاسب الآلي لا يضيف إلى السلوك غير المشروع جديدا، ولكن استخدام البيانات والمعلومات والبرامج هو الذي يمكن أن يضيف إلى الجريمة سمة الجريمة المعلوماتية (مطماطي ، 2019م).

ويعرّفها آخرون على أنّها: «جريمة ذات طابع مادي تتمثل في كل فعل أو سلوك غير مشروع، من خلال استعمال الوسائط الإلكترونية, حيث تتسبب في تحميل أو إمكانية تحميل المجني عليه خسارة, وحصول أو إمكانية حصول مرتكبه على أي مكسب، وتهدف هذه الجرائم إلى الوصول غير المشروع لبيانات سرية غير مسموح بالاطلاع عليها ونقلها ونسخها أو حذفها, أو تهديد وابتزاز الأشخاص والجهات المعنية بتلك المعلومات، أو تدمير بيانات وحواسيب الغير بواسطة فيروسات" (حفوظة، 2022).

وجلّ هذه التعريفات تعرضت للنقد من قبل الفقه، لذلك حاول جانب آخر من الفقه تعريف الجريمة الإلكترونية على نحو واسع من أجل محاولة تفادي أوجه القصور التي شابت تعريفات الإتجاه المضيق في التصدي لظاهرة الإجرام المعلوماتي (مطماطي، 2022).

ب. **تعريف الجريمة الإلـكترونية بمفهوم الواسع:**

من بين التعريفات الموسعة للجريمة المعلوماتية ما ذهب إليه من الفقه الأستاذ " هلالي عبد الله أحمد " بقوله: ″عمل أو امتناع عن عمل يأتيه الإنسان إضراراً بمكونات الحاسب وشبكات الإتصال الخاصة به، التي يحميها قانون العقوبات ويفرض للاعتداء عليها عقاباً".

وعرفتها منظمة التعاون الاقتصادي والتنمية {OCDE} بأنّها: " كل سلوك غير مشروع، أو غير أخلاقي أو غير مصرح به، يتعلق بالمعالجة الآلية للبيانات أو بنقلها " (مطماطي، 2022).

عرّفت في إطار المنظمات الأوروبية للتعاون والتنمية الاقتصادية: " كل فعل أو امتناع من شأنه أن يؤدّي على الاعتداء على الأموال المادية أو المعنوية، يكون ناتجاً بطريقة مباشرة عن تدخل التقنية المعلوماتية الإلكترونية " (ونوغي، وزيوش 2019، ص. 131).

ولقد عرّفها الدكتور " عبد الفتاح مراد " على أنّها :″ جميع الأفعال المخالفة للقانون والشريعة والتي ترتكب بواسطة الحاسب الآلي من خلال شبكة الانترنت، وهي تتطلب إلمام خاص بتقنيات الحاسب الآلي ونظم المعلومات سواء لارتكابها أو للتحقيق فيها، ويقصد بها أيضا أي نشاط غير مشروع ناشئ في مكوّن أو أكثر من مكوّنات الانترنت مثل مواقع الانترنت وغرف المحادثة أو البريد الالكتروني كما تسمّى كذلك في هذا الإطار بالجرائم السيبيرية أو السيبرانية لتعلقها بالعالم الافتراضي″، وهناك من يسمّيها أيضاً بجرائم التقنية العالية أو جرائم أصحاب الياقات البيضاء (حفوظة، 2022).

ونظراً لخطورة هذه الجريمة وآثارها الممتدة التي قد تصل من دولة لأخرى؛ فإنّ بعض الهيئات الدولية المعنية بجرائم الكمبيوتر، قد أرست قواعد لتعريف هذا النوع من الجرائم، من هذه الهيئات التي اتخذت التعريف التالي كتعريف لجريمة الكمبيوتر بأنّها: ″ أي سلوك غير قانوني أو غير قانوني أو غير أخلاقي أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر اعتداءا على الكمبيوتر" (مطماطي، 2022).

إنّ تجربة الأولية لبلد الجزائر لمواجهة الجريمة الالكترونية كانت خطوة أولى للحكومة الجزائرية لمواجهة ما يعرف بـ : " الجريمة الإلكترونية"، صدر سنة 2009م القانون رقم: 09-04 المؤرخ في: 05 أوت 2009م، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها (المادة 02، من القانون رقم: 04-9 المؤرخ في: 2009/08/16م)، إلا أنّ تجسيد بنوده على أرض الواقع ضعيف إلى حدّ الساعة، بعدما أهملت الجوانب التقنية الكفيلة بتصنيف هذه الجرائم وتحديد العقوبة المناسبة في حق مرتكبيها، واقتصرت العقوبات في أغلب الأحيان على الغرامة المالي.

ويتضمن القانون 19 مادة موزعة على 6 فصول، أعدّه نخبة من رجال القانون بمشاركة خبراء ومهنيين مختصين في مجال الإعلام الإلكتروني من كافة القطاعات المعنية، يتضمن القانون أحكاماً خاصة بمجال التطبيق وأخرى خاصة بمراقبة الاتصالات الإلكترونية، وعددت الحالات التي تسمح باللجوء إلى المراقبة الالكترونية، بالإضافة إلى القواعد الإجرائية المتضمنة تفتيش المنظومات المعلوماتية وكذا حجز

المعطيات المعلوماتية التي تكون مفيدة للكشف عن الجرائم الإلكترونية، ونص القانون في فصله الخامس على إنشاء الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، تتولى تنشيط وتنسيق عمليات الوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، ومساعدة السلطات القضائية ومصالح الشرطة القضائية في التحريات التي تجريها بشأن هذه الجرائم، وتتكفل أيضا بتبادل المعلومات مع نظيراتها في الخارج، قصد جمع كل المعطيات المفيدة في التعرف على مرتكبي الجرائم الإلكترونية وتحديد مكان تواجدهم، كما أنّ هذا القانون أكد في فصله الأخير على مبدأ التعاون والمساعدة القضائية الدولية من إطار مبدأ المعاملة بالمثل (حفوظة، 2022).

وفي نفس السياق، قال رئيس الكتلة البرلمانية لجبهة العدالة والتنمية لخضر بن خلاف، في تصريح خص به " يومية السلام اليوم " أنّ " مشكلتنا في قوانين سنّتها الحكومة فيما يخص الجريمة الإلكترونية ولم تطبّقها"، مضيفاً أنّ هناك مراسيم متعلقة بهذا القانون المصادق عليه سنة 2009م، لم تصدر لحد الساعة ولأسباب مجهولة، ما جعل حسبه، معالجة القضايا من هذا الشأن تصطدم بشبه فراغ قانوني، ما أدّى في عديد الحالات إلى استصدار أحكام وعقوبات تقريبية لا سند لها، كما دعا نفس المتحدث، الحكومة إلى ضرورة مراجعة موقفها تجاه هذا القانون، وقال: " لا بد من إيلائه أهمية أكبر في ظل دخول الشارع الجزائري نفق الإدمان، والاعتماد الرهيب على شبكة الإنترنت وما يصاحبها من آليات وخدمات إلكترونية، فضلا عن فتح مجال السمعي البصري، الذي يمكن أن يصطدم بمثل هذه الجرائم مستقبلا، مشددا في السياق ذاته على ضرورة تشريع قوانين جديدة تكرّس العقاب الصارم لكبح مثل هذه الجرائم التي وصفها بالخطيرة والمدمّرة.

وقد اصطلح المشرع الجزائري على تسمية الجرائم الالكترونية بالجرائم المتصلة بتكنولوجيات الإعلام والاتصال، وعرّفها بموجب المادة 02 من القانون رقم: 09-04 (المادة 02، من القانون رقم: 04-9 المؤرخ في: 2009/08/16م)، على أنّها:" جرائم المساس بأنظمة المعالجة الآلية للمعطيات الآلية المحددة في قانون العقوبات وأي جريمة أخرى ترتكب أو يسهل ارتكابها عن طريق منظومة معلوماتية أو نظام للاتصالات الالكترونية" (حفوظة،2022).

بعد التطرق إلى تعريف الجرائم الإلكترونية التي تعد إفرازا ونتاجا لتقنية المعلومات نخوض في البحث عن خصائص هذه الجريمة التي تميزها عن غيرها من الجرائم التقليدية أو المستحدثة بمجوعة من السمات قد يتطابق بعضها مع صفات أنواع أخرى من الجرائم هذا من ناحية، ومن ناحية أخرى؛ فإنّ اختلاف الجرائم المعلوماتية عن الجرائم التقليدية من حيث الأفعال الإجرامية أكسبها خصوصية غير عادية (مطماطي، 2022).

المطلب الثاني: خصائص الجرائم الإلكترونية وطبيعتها القانونية.

الفرع الأوّل: خصائص الجرائم الإلكترونية

نظراً لارتباط الجريمة الإلكترونية بجهاز الحاسوب، وشبكة الإنترنت بصفة عامّة، ووسائل التواصل الاجتماعي بصفة خاصة؛ فقد أضفى عليها ذلك مجموعة من الخصائص المميّزة لها عن خصائص الجريمة التقليدية، ومن بين هذه الخصائص ما يلي:

أوّلاً: جريمة عابرة للحدود.

أعطى انتشار شبكة الإنترنت إمكانية لربط أعداد هائلة من أجهزة الحاسوب المرتبطة بالشبكة العنكبوتية من غير أن تخضع لحدود الزمان والمكان، لذلك فإنّ من السهولة بمكان أن يكون المجرم في بلد ما والمجني عليه مقيم في بلد آخر (صهيب، وبشرى، 2021، ص 157)، وهنا تظهر الحاجة لوجود تنظيم قانوني دولي وداخلي متلائم معه لمكافحة مثل هذا النوع من الجرائم وضبط فاعليها (العجمي، 2014م، ص 20).

ثانياً: جريمة صعبة الإثبات والاكتشاف.

التباعد الجغرافي هو الذي يثير الإشكال بدايةً؛ والوسيلة المستخدمة لارتكاب الجريمة هي نبضة إلكترونية ينتهي دورها خلال أقلّ من ثانية واحدة، وكأن الجاني يقوم بتدمير الدليل بمجرّد استعماله، ويقوم بذلك بكلّ هدوء ودون إحداث أيّة ضجّة، وذلك على خلاف الكثير من الجرائم التي عرفها المجتمع عبر التاريخ (العجمي، 2014م، ص. 21).

المحور الثاني: مدى فعالية العقاب المقرّر لجريمة النصب والاحتيال الإلكتروني.

وفقاً لجسامة الجرائم المعلوماتية وخطورتها على الأفراد والمؤسسات والحكومات على حدّ سواء، بات لزاماً على المشرّع الجزائري الشروع في تعديل القوانين الإجرائية القاصرة في الكشف عن الجرائم المعلوماتية وفق ما يتماشى مع حداثة ومستجدّات الجريمة المعلوماتية، حيث تمّ تعديل قانون الإجراءات الجزائية من خلال القانون رقم: 04-15 المؤرخ في: 10 نوفمبر 2004م (قانون الإجراءات الجزائية، 2004م، ص ص 11 و12)، وكذا بالقانون رقم: 06-22 المؤرخ في: 20 ديسمبر 2006م (قانون رقم : 06-22، 2006م)، ومع تفشّي وضع الجريمة المعلوماتية، استحدث القانون رقم: 09-04 المؤرخ في: 05 أوت 2009م يتضمّن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتّصال. وعلى ضوء هذا المحور، سوف نتطرّق إلى دراسة العقوبات المقرّرة على الجريمة المعلوماتية في ظلّ التشريع الجزائري وهذا في المطلب الأوّل؛ والحماية القانونية في تصدّي الجريمة الإلكترونية في المطلب الثاني.

المطلب الأوّل: المسؤولية الجزائية المترتبة على الجريمة المعلوماتية في تقنين الجزائري.

للتطرّق إلى المسؤولية الجزائية الواقعة على مرتكبي الجرائم الإلكترونية، كان لزاماً توضيح دلالة المسؤولية، بمعنى التزام شخص بتحمّل النتائج التي تترتّب على سلوكه الذي ارتكبه مخالفاً به أصول أو قواعد قانونية، ومصطلح المسؤولية بشكلٍ عام ينطبق مع مفهوم المحاسبة وتحمّل الشخص لتبعة تصرّفاته وأفعاله؛ فيمكن أن يكون السلوك إيجابياً أم سلبياً مخالفاً لقواعد الأخلاق فحسب ولم يخالف فيها القواعد القانونية، وتقتصر آثارها على ما تثيره من استهجان واستغراب في نفوس أفراد المجتمع

لذلك السلوك المخالف للقواعد الأخلاقية (معتّز، 2014م، ص. 12)، كان السلوك ينطوي على مخالفة لقواعد قانونية؛ فإنّ المسؤولية هنا تكون مسؤولية قانونية ويتحمّل في هذه الحالة فرض جزاء قانوني تحدّده السلطة العامّة في الدولة.

وبهذا الصدد دلالة المسؤولية بناء على هذا التحديد تثير فكرة الخطأ وفكرة الجزاء، وهذه الأخيرة تنظّم الأفعال وتحمّل على العموم التزاماً أو جزاءاً قانونياً، نتيجة سلوك أو تصرّف يرتّب عليه القانون آثاراً وجزاءات معيّنة **(سويلم م، ، ص. 13).**

ومن هذا المنبر؛ فالمسؤولية الجزائية ينحصر تعريفها بأنّها: " التزام الإنسان بتحمّل الآثار القانونية المترتّبة على قيام فعل يعتبر من وجهة نظر القانون ونتيجة مخالفة هذا الالتزام هي العقوبة أو التدبير الاحترازي الذي يفرضه القانون على فاعل الجريمة أو المسؤول عنها " **(سويلم م.، المرجع نفسه، ص ص 13 و14).**

المطلب الثاني: الحماية القانونية في تصدّي الجريمة الإلكترونية.

أصبح الأمر جدّ صعب في تتبّع والكشف عن الجرائم الإلكترونية التي تعرف على أنّها : " كلّ فعل أو امتناع من شأنه الاعتداء على الأموال المادية والمعنوية يكون ناتجاً بطريقة مباشرة أو غير مباشرة في تدخّل التقنية المعلوماتية، وأمام قصور التقليدية في مواجهة الجريمة، كان لزاماً على المشرّع الجزائري التدخّل بنصوص آمرة لتجريم الظاهرة من جهة وإصدار قوانين خاصة تتلائم وطبيعة الجريمة ومستلزمات المكافحة التي تستدعي التعاون بين الجهات القانونية والمختّصين في المعلوماتية زيادةً على التعاون الدولي" (بوزنون، 2019، ص. 49).

الفرع الأول: القواعد الموضوعية المنظمة للجريمة الإلكترونية.

ولسدّ الفراغ أو الثغرة القانونية واقتداء بأغلب دول العالم (فشار، 2009)، قام المشرّع باستصدار قوانين معدّلة ومتمّمة لقانون العقوبات تارةً واستصدار قوانين خاصةً كان أهمّها على الإطلاق القانون رقم: 09-04 المؤرخ في: 05-08-2009م المتضمّن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها (القانون رقم: 90-04، 2009م، ص.ص. 05 و06).

أوّلاً: تعديل قانون العقوبات: استحدث المشرّع الجزائري القسم السابع مكرّر من قانون العقوبات من الفصل الثالث الخاص بجرائم الجنايات والجنح ضدّ الأموال تحت عنوان : " المساس بأنظمة المعالجة الآلية للمعطيات " (فرع ، 2017م، ص. 99) بنص المواد 394 مكرر إلى المادة 394 مكرر 07، وباستقراء هذه المادة يتّضح لنا أنّ المشرّع قسّم الجرائم الإلكترونية إل أربع طوائف تتعدّد بحسب المصالح المحمية التي تتمثّل أساساً في سرّية هذه المعطيات أو تكاملها وفي وفرتها وفي تكاملها هي:

- **الطائفة الأولى:** وتتضمّن جرائم الولوج إلى المعطيات المعالجة آليا عن طريق الغش والتزوير، وكذا جريمة الحذف؛ والتغيير؛ والتخريب في هذه المعطيات.

- **الطائفة الثانية:** الجرائم الإلكترونية بواسطة النظام المعلوماتي وأهمّها استعمال أو إفشاء أو نشر معلومات منصوص عليها في قانون العقوبات، وكذا البحث أو التجميع في معطيات مخزّنة في نظام معلوماتي.
- **الطائفة الثالثة:** الجرائم الإلكترونية المتعلّقة بأمن الدولة ومؤسساتها، كجرائم التجسّس والإرهاب.
- **الطائفة الرابعة:** الجرائم الإلكترونية للشخص المعنوي والتي تعادل عقوبتها خمس مرّات عقوبة الشخص الطبيعي المادة 394 مكرر 04 من قانون العقوبات (زعيطي، وبرناوي ، 2019م، ص. 233).

في سنة 2006م قام المشرّع بإدخال تعديلات جديدة مسّت القسم السابع مكرّر منه، حيث تمّ تشديد العقوبة على كلّ الجرائم الواردة في هذا القسم دون المساس بالجرائم الواردة فيها، ويعود ذلك بالتأكيد إلى إقرار المشرّع بأنّ الظاهرة جديدة ومستحدثة متميّزة عن الجرائم التقليدية (شنين، 2013م، ص. 11) من حيث محلّها وأشخاص مرتكبيها، وسعياً منه فيضمان المكافحة لم يميّز بين نوعية المعلومات التي تطالها الحماية سواء كانت مادية أو اقتصادية أو مسائل أمنية غرضه في ذلك هو حتماً تحقيق الردع العام على أثر التزايد الخطير لنسب الجرائم المرتكبة وتنوعها وخطورتها على الأفراد من جهة وعلى الإقتصاد الوطني من جهة أخرى (بوزنون ، 2019، ص.49).

ثانياً: القانون الخاص بالوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال.

تواكباً مع التطوّرات التي عرفتها الجزائر في مجال تطوّر التقنية والتكنولوجيا؛ ولأنّها في الغالب أصبحت محلا للجريمة باشر المشرّع الجزائري إجراءات جديدة للمواجهة تضمّنت إصدار القانون رقم: 04-09 المتضمّن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال ومكافحتها، وهو القانون المنظّم لفضاء المعلوماتية بصفة عامّة ومكافحة المجال الإجرامي المتّصل بها من خلال قواعد تسمح بمتابعة هذا النوع من الجرائم ومرتكبيها بشكلٍ بشكل يضمن شرعية الإجراءات المتّخذة.

إنّ الظاهر من النص يوحي بأنّ القانون يتضمّن انتهاك صارخ للحق في الخصوصية، ولكن الواضح أنّ هناك ما يبرّره في الغالب وهو مضمون المادة 04 من القانون رقم: 90-04 التي نصّت على أربع حالات يجوز فيها فقط اللّجوء إلى هذا الإجراء، وذلك بالنظر إلى خطورة التهديدات المحتملة ولأهمية المصلحة المحمية منها:

- ✓ جرائم الإرهاب والتخريب وجرائم ضدّ امن الدولة.
- ✓ عندما تتوفّر معلومات عن احتمال وقوع اعتداء على منظومة معلوماتية تهدّد مؤسسات الدولة أو الدفاع الوطني.
- ✓ لضرورات التحقيق والمعلومات القضائية.
- ✓ في إطار تنفيذ طلبات المساعدات القضائية بين الدول (شيخ، وشيخ ، دون سنة،).

الفرع الثاني: القواعد الإجرائية المنظّمة لمكافحة الجريمة المعلوماتية.

حيث خصّ المشرّع الجزائري هذه الجرائم بجملة من الإجراءات الخاصة تمسّ كل من مرحلة البحث والتحرّي؛ التحقيق والمحاكمة، وتكمن خصوصية إجراءات المتابعة في الجريمة الإلكترونية فيما يلي:

أوّلاً: تمديد الاختصاص المحلي.

تمديد الاختصاص المحلي لكل من ضباط الشرطة القضائية؛ وقاضي التحقيق؛ ووكيل الجمهورية؛ المادة 37 من قانون إجراءات جزائية إذا تعلّق الأمر بالجريمة المنظمة وجرائم المعالجة الآلية للمعطيات؛ الإرهاب؛ تبييض الأموال؛ وجرائم الصرف.

كذلك نظّم المشرّع الجزائري في القانون رقم: 09-04 المؤرخ في: 05 أوت 2009م، أحكاماً جديدة خاصة بالاختصاص في مجال بالجريمة المعلوماتية تتماشى والتطور الذي لحق الجريمة، من هذه القواعد ما نصّت عليه المادة 03 التي تضمّنت الإجراءات الجديدة التي تتطلّبها التحرّيات والتحقيقات من ترتيبات تقنية؛ بالإضافة إلى ذلك قرّرت المادة 15 من القانون رقم: 09-04 على أنّه : " زيادة على قواعد الاختصاص المنصوص عليها في قانون الإجراءات الجزائية، تختّص المحاكم الجزائرية بالنظر في الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال المرتكبة خارج الإقليم الوطني عندما يكون مرتكبها أجنبياً، وتستهدف مؤسسات الدولة الجزائرية والدفاع الوطني أو المصالح الإستراتيجية للاقتصاد الوطني ".

ثانياً: إمكانيات التحرّي والكشف.

إنّ أهمية جهاز الشرطة القضائية في الكشف عن الجريمة الإلكترونية، والتعرّف على المجرم الإلكتروني. وما تجدر الإشارة إليه أنّ هذه الإمكانيات لا يرخّص بها إلاّ في بعض الجرائم المعيّنة من طرف المشرّع الجزائري على سبيل الحصر لا المثال بما فيها الجريمة الإلكترونية استدركها المشرّع بموجب تعديل قانون الإجراءات الجزائية القانون رقم: 06-22 والتي تتمثّل في:

- ✓ اعتراض المراسلات (براهيمي ، د.ت.، ص. 139) التي تتم عن طريق وسائل الاتّصال السلكية واللاسلكية.
- ✓ وضع الترتيبات التقنية دون موافقة المعنيين من أجل التقاط وتثبيت وتسجيل الكلام المتفوّه به بصفة خاصة أو سرّية من طرف شخص أو عدّة أشخاص في أماكن خاصة (بوقرين، 2019، ص. 382).

- جواز التسرّب أو الاختراق للكشف عن الجريمة الإلكترونية بمقتضى المادة 65 مكرر 12 من القانون رقم: 06-22 المتضمّن قانون العقوبات؛ ولأنّه إجراء غير مألوف وخطير في عمل سلطات الضبط القضائي أحاطه المشرّع بجملة من الضوابط أهمّها: الإذن القضائي بالتسرّب من وكيل الجمهورية أو قاضي التحقيق المادة 65 مكرر 11 وأيضاً احترام المدّة القانونية للتسرّب.

ثالثاً: التفتيش والتوقيف تحت النظّر.

فقد نصّ المشرّع الجزائري في المادة 47/04 من قانون الإجراءات الجزائية الجزائري بإمكانية التفتيش والضبط على المكوّنات المعنوية للحاسوب، بنصّه على أنّه: " إذا تعلّق الأمر بجريمة ماسّة بأنظمة المعالجة الآلية للمعطيات يمكن لقاضي التحقيق أن يقوم بأيّة عملية تفتيش أو حجز ليلاً أو نهاراً وفي أي مكان على امتداد التراب الوطني أو يأمر ضباط الشرطة القضائية للقيام بذلك".

فإذا تعلّق الأمر بالجريمة الإلكترونية طبقاً لنص المادة 51/05 من الأمر رقم: 15-02 المؤرخ في: 23 جويلية 2015م، (الأمر رقم: 15-02، 2015م، ص. 28) مع العلم أنّ هذا الإجراء بوليسي يقوم به الضابط ضدّ كلّ شخص تتوافر دلائل قوّية على ارتكابه الجريمة في الجريمة المتلبّس بها بوضع شخص في مركز الشرطة أو الدرك لمدّة يحدّدها المشرّع كلّما دعته الضرورة لذلك، على أنّه لا يجوز أن تتجاوز مدّة التوقيف للنظر ثمان وأربعون (48) ساعة ما عدا بعض الجرائم الخطيرة التي خصّها المشرّع باستثناءات.

الفرع الثالث: الهياكل الخاصة لمواجهة الجرائم المعلوماتية.

عمدت معظم الدول إلى استحداث وحدات خاصة لمكافحة هذا النوع من الجرائم، كما تمّ إنشاء أجهزة متخصّصة على المستوى الدولي مهمّتها البحث والتحرّي في العالم الافتراضي على غرار هيئة " الإنتربول؛ واليوروبول؛ والافريبول". أمّا في الجزائر؛ فقد تمّ تسخير هيئات ووحدات متخصّصة أبرزها: " الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتّصال؛ إضافةً إلى وحدات قضائية وأخرى تابعة لسلك الأمن والدرك الوطني ".

أوّلاً: الهيئات الفنّية المتخصّصة في البحث والتحري عن الجرائم الإلكترونية.

وهي وحدات التي تسند لها مهام الوقاية ومكافحة الجرائم الإلكترونية بالنظر إلى تشكيلها البشرية الخاصة التي تضم محققين من نوع خاص.

أ. الهيئة الوطنية للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام الاتّصال.

أنشأت الهيئة في الجزائر بموجب المادة من القانون رقم: 09-04 المتضمّن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيا الإعلام والاتصال ومكافحتها وتحديداً بنص المادة 13 منه، لكنّه ترك أمر تحديد تشكيلة الهيئة وتنظيمها وكيفيات سيرها للتنظيم الصادر بموجب المرسوم الرئاسي رقم: 15-261.

ب. الوحدات التابعة لسلك الأمن الوطني.

توجد على مستوى جهاز الأمن الوطني ثلاث (03) وحدات مكلّفة بالبحث والتحقيق في الجرائم المعلوماتية، وهي كالتالي:

- ✓ المخبر المركزي للشرطة العلمية بـ: الجزائر العاصمة.
- ✓ المخبر الجهوي للشرطة العلمية بـ: قسنطينة.
- ✓ المخبر الجهوي للشرطة العلمية بـ: وهران (رابح ، 2014، ص. 322).

ج. **الوحدات التابعة للقيادة العامّة للدرك الوطني.**

أهم الوحدات التابعة للدرك الوطني والمكلّفة بالبحث والتحقيق في الجرائم المعلوماتية على المستوى المركزي، نجد المعهد الوطني للأدلّة الجنائية وعلم الإجرام والكائن مقرّه في: بوشاوي، وهو مؤسسة وطنية ذات طابع إداري تم إنشاءه بموجب المرسوم الرئاسي رقم: 04-183 المؤرخ في: 26 جوان 2004م (مرسوم رئاسي، 2004م، ص 18).

الفرع الرابع: الهيئات القضائية الخاصة للبتّ في الجرائم الإلكترونية.

عكف المشرّع الجزائري وقبله التشريعات المقارنة خاصةً المشرّع الفرنسي إلى استحداث الأقطاب الجزائية المتخصّصة، وهي محاكم ذات اختصاص إقليمي موسّع بموجب القانون رقم: 04-14 المؤرخ في: 10 نوفمبر 2004م المعدّل والمتمم لقانون الإجراءات الجزائية الجزائري الذي أجاز توسيع اختصاص بعض المحاكم (بولحية، ووسيح ، 2019، ص. 46) ووكلاء الجمهورية وقضاة التحقيق في جرائم محدّدة على سبيل الحصر، وتوصف أنّها خطيرة وعلى درجة عالية من التعقيد والتنظيم، وهي: جرائم المخدّرات؛ الجريمة المنظمة عبر الحدود الوطنية، الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات؛ تبييض الأموال؛ الجرائم الإرهابية والتخريبية؛ وجريمة مخالفة التشريع الخاص بالصرف.

ولقد تمّ بالفعل صدور النص التنظيمي الخاص الذي مدّد الاختصاص لأربع (04) جهات قضائية، المرسوم رقم: 06-348 المؤرخ في: 2006/10/05م المعدّل والمتمّم بالمرسوم التنفيذي رقم: 16-267 المؤرخ في: 17 أكتوبر 2016م والذي بموجبه تحديد هذه المحاكم مع تعديل طفيف في المرسوم التعديل (مرسوم تنفيذي رقم : 16-267، 2016)، بحيث شمل التقسيم إضافةً بعض المجالس القضائية بمقتضى المادة 03؛ و04؛ و05 المعدّلة للمواد 03؛ و04؛ و05 من المرسوم السابق.

ونظراً لكون المشرّع الجزائري لم يورد نصوصاً خاصة لتجريم الاحتيال أو النصب الإلكتروني؛ فإنّنا نطبّق على الجريمة القواعد العامّة لجريمة النصب وفقاً للمادتين 372؛ و373 من قانون العقوبات الجزائري (العايب، وعرابة، 2021م، ص ص. 229 -243).

خاتمة:

أصبح العالم اليوم يعيش ثورة ثالثة، أو الموجة الثالثة كما يسميها البعض وهي ثورة تكنولوجيا المعلومات والمعرفة والتي أصبحت أساساً للتنمية وزيادة الإنتاج، وسرعة اتخاذ القرار الصحيح، وقد تمخض عن هذا التطور انتشار ما يعرف بـ: " الجريمة الالكترونية " والتي تتمتع بطبيعة قانونية خاصة تميزها عن الجريمة التقليدية.

وقد حاول المشرع الجزائري جاهداً للتصدي لهذا النوع من الجرائم ومكافحتها بشتى الطرق، من خلال سن بعض القوانين وكذا تعديل البعض الآخر منها كقانون العقوبات وكذا قانون الإجراءات الجزائية؛ وبالرغم من الأساليب الوقائية والردعية المعتمدة في الجزائر ومجموع القوانين والتنظيمات

الصادرة في هذا الشأن تبقى المواجهة صعبة في ظلّ عدم تهيئة الأسس القاعدية التقنية الكفيلة بالتحقيق؛ والبحث؛ وتصنيف درجات الجريمة قبل إصدار العقوبة.

وفي الأخير نتوصل إلى النتائج التالية:

تواجد فروقات في توحيد تعريف الجريمة الإلكترونية دلالة على أنّه عنصر افتراضي غير ملموس وغير متحكّم فيه وعدم إمكانية تصدّي له ومكافحته بالإثبات نادراً.

قصور وتعثّر القوانين التقليدية على تولّي زمام هذه الجريمة المستحدثة.

رغم القوانين التي سنها المشرع إلا أنها تبقى قليلة ولا تجاري التطور الذي تعرفه الشبكة العنكبوتية من تطور.

وبالنسبة للاقتراحات:

- ✓ على المشرع الجزائري أن يضع نصوصاً قانونية مستحدثة حسب تبلور التكنولوجيا.
- ✓ عقد دورات تدريبية التي تعتني بمكافحة الجرائم الإلكترونية- تكمن في إنشاء فئة متخصصة من الطاقم الأمني الإلكتروني يهتّم في حصر الجرائم الإلكترونية في قبضته.
- ✓ إنشاء مدرسة مختصة في مجال تكوين رجال شرطة متخصصين وقضاة في مجال مكافحة هذا النوع من الجرائم من حيث الممارسة العملية والتطبيقية، وليس من خلال الممارسة التشريعية التنفيذية.
- ✓ صنع فئة من قضاة متمكّنة في مجال مكافحة هذا النوع من الجرائم من حيث الممارسة التشريعية التنفيذية.

قائمة المصادر والمراجع:

1) أبو سويلم، معتّز حمد الله، (2014م)، المسؤولية الجزائية عن الجرائم المحتملة، رسالة ماجستير مقدّمة استكمالاً للحصول على درجة الماجستير في القانون العام، قسم القانون العام، كلية الحقوق، جامعة الشرق الأوسط.

2) الأمر رقم: 15-02 مؤرخ في: 07 شوّال عام 1436هـ الموافق لـ 23 يوليو سنة 2015م، يعدّل ويتمّم الأمر رقم: 66-155 المؤرخ في: 18 صفر عام 1386هـ الموافق لـ 08 يونيو سنة 1966م والمتضمّن قانون الإجراءات الجزائية، جريدة رسمية، العدد 40.

3) براهيمي، جمال، (دون سنة)، مكافحة الجرائم الإلكترونية في التشريع الجزائري، المجلة النقدية، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، تيزي وزو.

4) بوزنون، سعيدة، (ديسمبر، 2019)، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة العلوم الإنسانية، المجلد: ب، العدد 52، كلية الحقوق، جامعة الإخوة منتوري، قسنطينة.

5) بوضياف، إسمهان، (سبتمبر 2018م)، الجريمة الإلكترونية والإجراءات التشريعية لمواجهتها في الجزائر، مجلة الأستاذ الباحث للدراسات القانونية والسياسية، العدد الحادي عشر، جامعة محمد بوضياف، المسيلة.

6) بوقرين عبد الحليم، (شوال 1440هـ / يونيو 2019م)، المسؤولية الجنائية عن الاستخدام غير المشروع لمواقع التواصل الاجتماعي: دراسة مقارنة، مجلة جامعة الشارقة للعلوم القانونية، دورية علمية محكمة، المجلد: 16، العدد: 01، كلية الحقوق والعلوم السياسية، جامعة عمار ثليجي، الأغواط، الجزائر.

7) بولحية، شهيرة، ووسيح، دنيا زاد، (ديسمبر 2019م)، الاحتيال الإلكتروني، مجلة الدراسات القانونية والاقتصادية، العدد: 04، المركز الجامعي سي الحواس، بريكة، باتنة.

8) حفوظة، الأمير عبد القادر، (2022)، الجريمة الإلكترونية وآليات التصدّي لها، الموسوعة الجزائرية، للدراسات السياسية والإستراتيجية، جامعة أبو بكر بلقايد، تلمسان، على الساعة : 22:54 مساءاً، يوم: 11 مارس 2022م، نقلاً عن الموقع الإلكتروني : https://www.politics-dz.com

9) رابح، وهيبة، (ديسمبر 2014م)، الجريمة المعلوماتية في التشريع المعلوماتية في التشريع الإجرائي الجزائري، مجلة الباحث للدراسات الأكاديمية، العدد04، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد ابن باديس، مستغانم.

10) زعيطي، آمنة، وبرناوي، راضية، (2019/06/01م)، مكافحة الجرائم الإلكترونية في ضوء قانون العقوبات الجزائري – دراسة مقارنة، مجلة حقوق الإنسان والحريات العامة، مجلة دولية محكمة نصف سنوية، مجلد:04، العدد: 07، جامعة مستغانم.

11) شاهين، صهيب، ياسر محمد، وأوترابي، بشرى، محمد حسن ، (2021م) ، الجريمة الإلكترونية وبعدها القانوني – دراسة مقارنة بين التشريع الجزائري والفلسطيني، مجلة نوميروس الأكاديمية، المجلد الثاني، العدد الأول، جامعة عباس لغرور، خنشلة.

12) شنين، صالح، (2012م/ 2013م) ، الحماية الجنائية للتجارة الإلكترونية – دراسة مقارنة، رسالة لنيل شهادة الدكتوراه في القانون الخاص، كلية الحقوق، جامعة أبو بكر بلقايد، تلمسان.

13) شيخ، سناء، وشيخ، محمد زكرياء، (د.ت.)، مكافحة الجرائم الإلكترونية في القانون الجزائري، دون بلد.
ظ

14) العايب، سامية، وعرابة، منال، (2021)، الحماية الجزائية للمستهلك من جريمة النصب الإلكتروني، مجلة هيرودوت للعلوم الإنسانية والاجتماعية، المجلد 05، العدد 03، مخبر الدراسات القانونية البيئية، كلية الحقوق والعلوم السياسية، جامعة 08 ماي 1945م، قالمة، الجزائر.

15) العجمي، عبد الله دغش، (2014م)، المشكلات العملية والقانونية للجرائم الإلكترونية – دراسة مقارنة، قدّمت هذه الرسالة استكمالاً للحصول على درجة الماجستير في القانون العام، جامعة الشرق الأوسط.

16) فرع، أبي سمراء، (24و25 مارس، 2017)، الجرائم الإلكترونية، أعمال المؤتمرات، المؤتمر الدولي الرابع عشر، لبنان/ طرابلس

17) فشار عطاء الله، أكتوبر 2009م، مواجهة الجريمة المعلوماتية في التشريع الجزائري، بحث مقدّم إلى الملتقى المغاربي حول القانون والمعلوماتية، المزمع عقده بأكاديمية الدراسات العليا بليبيا في أكتوبر 2009م، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور بالجلفة.

18) قانون العقوبات الجزائري، (2021)، والمتعلّق بجريمة القذف والسب إزاء رئيس الجمهورية أو فيما يخص دين الاسلام، أو ضدّ الهيئات العمومية

19) القانون رقم: 04 –15 المؤرخ في: 10 نوفمبر 2004م المعدل والمتمم لقانون العقوبات، الجريدة الرسمية العدد: 44.

20) قانون رقم 06-22 مؤرخ في: 29 ذي القعدة عام 1427ه الموافق لـ 20ديسمبر سنة 2006م، يعدل ويتمم الأمر رقم: 66-155 المؤرخ في: 18 صفر عام 1386ه الموافق لـ 8 يونيو سنة 1966م والمتضمن قانون الإجراءات الجزائية.

21) القانون رقم: 04-14 المؤرخ في: 27 رمضان عام 1425ه الموافق لـ 10 نوفمبر سنة 2004م الموافق لـ 10 نوفمبر سنة 2004م المعدل والمتمم للأمر رقم: 66-155 المتضمن قانون الإجراءات الجزائية، جريدة الرسمية، عدد: 71 بتاريخ: 10 نوفمبر 2004م.

22) القانون رقم: 09-04 مؤرخ في: 14 شعبان عام 1430ه الموافق لـ 05 غشت سنة 2009م، يتضمّن القواعد الخاصة للوقاية من الجرائم المتّصلة بتكنولوجيات الإعلام والاتّصال ومكافحتها، جريدة الرسمية، العدد: 47.

23) القانون رقم: 04-09 المؤرخ في: 25 شعبان 1430ه الموافق لـ 16 أوت 2009م المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، جريدة الرسمية، العدد 47.

24) مرسوم تنفيذي رقم: 16-267 مؤرخ في: 17 أكتوبر 2016م، الجريدة الرسمية، عدد: 62، مؤرخة في: 23 أكتوبر 2016م، ص 10. إذ يعدلّ بالمرسوم التنفيذي رقم: 06-348 المؤرخ في: 05 أكتوبر سنة 2006م والمتضمّن تمديد الاختصاص المحلي لبعض المحاكم ووكلاء الجمهورية وقضاة التحقيق.

25) مرسوم رئاسي رقم: 04-183 ممضي في: 26 يونيو 2004م، يتضمّن إحداث المعهد الوطني للأدلّة الجنائية وعلم الإجرام للدرك الوطني وتحديد قانونه الأساسي، جريدة رسمية، رقم: 41 مؤرخة في: 27 يونيو 2004م.

26) مطماطي، راوية، (2019م)، الجريمة الإلكترونية في التشريع الجزائري، مجلة القانون والأعمال الدولية، كلية الحقوق والعلوم السياسية، جامعة عبد الحميد بن باديس، مستغانم، الجزائر، 2019/04/17م، على الساعة: 18:09 مساءاً، يوم: 11 مارس 2022م، نقلاً عن الموقع
https://www.droitetentreprise.com

27) نمديلي، رحيمة، (2022)، خصوصية الجريمة الإلكتروني في القانون الجزائري والقوانين المقارنة، مركز جيل البحث العلمي، مؤسسة علمية خاصة ومستقلّة، 2017/04/08م، كلية الحقوق والعلوم السياسية جامعة محمد لمين دباغين سطيف 2 الجزائر. كتاب أعمال مؤتمر الجرائم الإلكترونية المنعقد في طرابلس/ لبنان، يومي 24-25|03|2017، على الساعة: 19:22 مساءاً، يوم: 2022/03/11م، نقلاً عن الموقع الإلكتروني: *https://jilrc.com*

أسباب الجريمة الالكترونية من منظور سوسيو أنثروبولوجي

Causes of cybercrime from a socio-anthropological perspective

ط. د.زغودة بورشــاق/ جامعة عنابة/الجزائر

PhD. Zagouda Bourechak/ Annaba University/ Algeria

ملخص الدراسة:

تعتبر الجريمة الالكترونية إحدى نتاج أليات العولمة والتطور الكبير لوسائل الإعلام وتكنولوجية الاتصال، والذي تمخض عنه نوع جديد من الجرائم له طبيعته وأسبابه وخصائصه التي تميزه عن الجرائم التقليدية.

والملاحظ أن أغلب الدراسات التي عالجت الجريمة الإلكترونية تناولتها من جانب واحد (القانوني). في حين أن النظرة الاجتماعية والأنثروبولوجية، لم تستوف حقها في الدراسة والبحث العلمي. رغم أهميتها الدلالية التي تعكس سمات الإجرام الإلكتروني، وعلاقتها بالتركيبة البنيوية للبيئة الافتراضية والمجرم الإلكتروني ومسبباته المختلفة (سوسيو، نفسية. تكنولوجية ...إلخ)

لذا سنحاول في هذه المداخلة الإحاطة بأهم العوامل والأسباب المؤدية للجريمة الإلكترونية (النفسية والاجتماعية، والاقتصادية والسياسية، وتقنية). بنوع من التفصيل، وفق نظرة سوسيو أنتروبولجية.

الكلمات المفتاحية: الجريمة، الجريمة الالكترونية، الأسباب، المعلوماتية، الحاسوب.

Abstract:

Cyber crime is a product of the mechanisms of globalization and the great development of the media and communication technology, which has resulted in a new type of crime with its nature, causes and characteristics that distinguish it from traditional crimes.

It is noted that most of the studies dealing with cybercrime have been conducted unilaterally (legal). While the social and anthropological view did not fulfil its right to study and scientific research. Despite its semantic importance, which reflects the features of cyber crime, its relationship to the structural composition of the virtual environment and the cyber criminal and its various causes (Susio, Psycho). technology, etc.).

In this intervention we will try to identify the main factors and causes of cybercrime (psychological, social, economic, political and technical). In some sort of detail, ... According to susio entropolism.

Keywords: Crime, Cyber Crime, Causes, Informatics, Computer.

مقدمة:

الجريمة ظاهرة اجتماعية قديمة قدم المجتمعات الانسانية. حيث نشأت في المجتمعات القديمة وفي ظل ظروف طبيعية معينة وثقافة بيئية واجتماعية وصراعات مختلفة، أدت إلى نشوء فعل الجريمة على يد الإنسان ككائن بيولوجي وأنثروبولوجي واجتماعي. يبحث فيه عن ذاتيته، وغذائه ومكانته بين أفراد قبيلته.

إن ظهور الجريمة في المجتمعات الحديثة والمعاصرة لها امتدادها في التاريخ السوسيو أنثروبولوجي للإنسان وتركيبته البنيوية والاجتماعية والثقافية، التي أعطت للفعل الإجرامي أبعاد مترامية في كنه الظاهرة المدروسة "الجريمة " وانعكاساتها على المدى الطويل على التركيبة النسقية للفرد والمجتمع، وعلى نوع الإجرام وأساليبه المتنوعة وعلى المجرم في بيئته الاجتماعية. لذا تعمل الترابطية التكاملية بين تدفق العناصر السلبية والإيجابية في البناء الوظيفي لتشكل من خلاله التشكيلات الاجتماعية والمؤسساتية من منظور الما كرو وميكرو سوسيولوجي، الذي يؤسس لنمط جديد للسلوك الإجرامي المقنن والمنظم في ظل العولمة الكاسحة لثقافة المجتمعات.

تجعلنا ننظر لظاهرة الجريمة بمفهومها التقليدي والمستحدث والمنحى الذي أخذته، وتركيبة الانسان المبتكر للفعل الاجرامي وطبيعة الاختراعات الكونية في ظل البيئة الواقعية والافتراضية له دلالات سوسيو أنثروبولوجي في النظام الرقمي والالكتروني. حينما يفرض الاعلام المعولم في قالبه الإلكتروني سلعته المادية لصناعة المجرم والجريمة المستحدثة والمنظمة لتكون أكثر تعقيدا وأكثر خطرا على الأفراد والدولة.

وأمام التطور الكبير الذي تشهده المجتمعات المعاصرة والانتشار الواسع للوسائل التكنولوجية الحديثة والتدفق السريع للمعلومات، ضمن نظام الشبكات والحاسوب الآلي أو الهواتف الذكية أدى لتبلور مفهوم جديد "الجريمة" باكتساحها عالم تكنولوجية الإعلام والاتصال. أين أطلق عليها مسميات عدة "جريمة المعلومات "أو "جريمة الحاسب، أوجريمة نظام الحاسوب" أو "الجريمة الالكترونية ". والتي تعتبر إحدى نواتج العولمة الثقافية وتطور تكنولوجية الإعلام والاتصال.

إن انتشار الجريمة الالكترونية وتشعب أساليها وتزايد معدلاتها في كل أنحاء العالم، له عدة أسباب وعوامل متداخلة ومعقدة التي تعمل كمحرك ديناميكي للفاعلين والمجرمين لإتيانها، وذلك تحت وطأة أهداف وغايات مرسومة وإن تباينت. فإن الفعل حتما يؤدي إلى الجريمة الالكترونية بمدلولها السوسيو أنثروبولوجي والنفسي. بأركانها القانونية كما لها انعكاساتها أو تداعياتها على الأفراد والمجتمع، والذي ينبأ بالخطر المحدق بكيان الدول والمجتمعات، وبحجم الدمار والخراب الذي يصيب مؤسسات الدولة العامة والخاصة والأكاديمية، مما يستدعي تكاثف الجهود من أجل الحد من خطورتها على المدى البعيد.

أولا: مشكلة الدراسة

الجريمة الالكترونية ظاهرة عالمية مست كل الدولة. وأن الالمام بمفهوم الجريمة المعولمة وخصائصها ومسبباتها، وعلاقتها بالوسيلة التكنولوجية والفضاء الافتراضي تعطي رؤية بنائية وظيفية ذات أبعاد مختلفة قد تتشابك مع نظرة أنثروبولوجيا الجريمة في امتداد بنية العلاقات الثلاثية (البنية المرفولوجية، نفسية، ثقافية،

اجتماعية، تكنولوجية). وتفاعلية البيئة الإيكولوجية والافتراضية وثنائية الكائن الانساني والاعلام المعولم وتشكلاته. تخلق مبررات ودعائم تتجسد من خلالها القوة، والخضوع والسيطرة من خلال قراءة أنثروبولوجية لوقائع المجتمعات البدائية و حركية التغيير الأثنوغرافي للمجتمعات والتطور التكنولوجي المبني على كيفية السيطرة والخضوع من منظور التأريخ والسوسيو أنثروبولوجي لابن خلدون في عملية مواكبة الانسان والتطور العمراني والملك والدولة. التي تعطي مقاصد ومعنى لمفهوم ماهية الجريمة الإلكترونية. ومن ثم نشوء الجريمة الإلكترونية وتطورها وتشعب ميادينه وانتشارها، مرتكزة في البحث في ماهيتها ومدى ارتباطها بالواقع الفعلي للإجرام المعاصر في ظل العولمة واختلاف التوجهات والرؤى. وعلى الرغم من اختلاف بؤر الإجرام الإلكتروني وتباين نوع الجريمة ومرتكبها. إلاّ أن الأسباب والعوامل المؤدية إلى نوع معين من الإجرام الإلكتروني أو المعلوماتي يختلف باختلاف الذات أو الشخصية الإجرامية وخبرتها أو اختلاف الهدف والغاية من وراء الفعل، وقدرة تخفي آثارها. والذي يجعلنا نتوجه في طرحنا إلى تحديد المفهوم الدلالي للجريمة الالكترونية وخصائصها كي نستوعب أكثر الرؤية الأنثروبولوجية في تحديد بعض عوامل ومسببات الجريمة بأبعاد متباينة. تقودنا إلى طرح التساؤلين: ما مفهوم الجريمة الإلكترونية؟ ماهي عوامل ومسببات الجريمة الالكترونية؟

ويكمن الهدف من هذا العمل البحثي نوجزه في ثلاث نقاط: تحديد مفهوم الجريمة الالكترونية، تحديد أهم الأسباب والعوامل التي نعتقد أن لها دخل في استفحال الجريمة الإلكترونية، التأسيس النظري للموضوع من منظور سوسيو أنثروبولوجي.

ونستقي أهمية الدراسة من أهمية الموضوع المعالج، باعتباره يعالج ظاهرة خطيرة أفرزتها وسائل العولمة وتحدياتها. وأن الدراسة من منظور أنثروبولوجي تعطي الاحاطة بعدة عوامل (ايكولوجية، نفسية، ثقافية، اجتماعية، إعلامية). على غرار الطرح القانوني الذي يهتم بالنهج القانوني والجنائي للجريمة.

وللإجابة على هذا التساؤل سنتناول الموضوع وفق الخطة التالية: - أولا - تحليل مفاهيمي ،- الخصائص الجريمة الإلكترونية - أنواعها. ثانيا - المعالجة النظرية للموضوع ، - الأسباب والعوامل الذاتية والنفسية – الاسباب الخارجية وفي الأخير نختم العمل بخاتمة وجملة من التوصيات وقائمة المراجع

ثانيا: تحليل مفاهيمي:

تعتبر الجريمة الالكترونية هي إحدى صور الاجرام المستحدث. حيث أنه لا يوجد تعريف دقيق للجريمة له دلالة علمية واضحة تعطي وضوح للمفهوم، بل هناك جملة من التعاريف التي تطرقت أغلبها للجانب الالكتروني أو المعلوماتي للحاسب الآلي كوسيلة للتعريف بالجريمة (نظام الحاسوب أو شبكة الحاسوب). أي اجتياح الجريمة عالم المعلوماتية في البيئة الالكترونية أو الافتراضية، حينئذ سميت الجريمة ب "الجريمة الالكترونية " "كجريمة الاحتيال الالكتروني"، "وجريمة التقنية العالية "، "جرائم هاكرز" و"جرائم الحرب الإلكترونية" وجرائم دعارة الاطفال، والارهاب...إلخ. ولقد أطلق تسمية الجريمة الإلكترونية كتعبير علائقي ارتباطي بالأداة المستعملة في الجريمة. سنتناول في البداية بناء تحليلي للمفاهيم الواردة في هذه الدراسة.

1 -الجريمة: وهي " أي فعل يحدث أذى أو ضررا بين الآخرين أو هي سلوك يسبب خروجا على قوانين المجتمع، وخرقا لتقاليد ويقابل المجتمع هذا السلوك أو العمل بالجزاء" (سليم، 1981، ص.218). وعرفها الانثروبولوجي راد كليف بروان بأنها "انتهاك للعرف السائد مما يستوجب توقيع الجزاء على منهكيه (عبد الخالق، ورمضان، 2001، ص. 84).

وفي علم الاجتماع الجريمة هي الفعل الذي يصطدم بالضمير الجمعي للمجتمع. حسب ما ذهب إليه دوركايم فيقابله رد فعل (المشيخص، 2005، ص.13). وجاء تعريف الجريمة أيضا في الشريعة أنها " المحظورات شرعا في إتيان فعل منهي عنه أوترك فعل مأمور به، وأصل الكلمة من جرم أي كسب قطع. "(المشيخص، 2005، ص. 11). وحسب التعاريف السابقة التي تتفق في أغلبها أن الجريمة هي الفعل أو السلوك المنحرف والخارج عن القانون وقيم المجتمع وسلوكات الجماعة، والذي يتسبب في أضرار كبيرة على الأفراد والمجتمع.

ولقد وردت كلمة جريمة والمجرمون في كثير من المواضع في القرآن الكريم نذكر منها قول الله تعالى"ويَا قَومِ لاَ يَجْرِمَنَّكُمْ شِقَاقِيَ أَنْ يُصِيبَكُمْ مِّثْلُ مَا أَصَابَ قَوْمَ نُوحٍ أَوْ قَوْمَ هُودٍ أَوْ قَوْمَ صَالِحٍ. وَمَا قَوْمُ لُوطٍ مِّنكُم بِبَعِيدٍ"(القرآن الكريم: سورة هود، **الآية 89**). وقول تعالى "إنّ الّذِينَ أَجْرَمُوا كَانُوا مِنَ الّذِينَ ءامَنُوا يَضْحَكوُنَ"(القرآن الكريم سورة المطففين، الآية 29). وأيضا قول الله تعالى " وماَ أَضَلَّناَ إلاَّ المُجْرِمُونَ"(القرآن الكريم: سورة الشعراء، الآية 99).

وعليه الجريمة من الناحية الشرعية هي إتيان الفعل المنافي لشريعة الله وفطرة الانسان المبنية على السريرة السليمة، والفعل السليم المتفق والشرع والعرف الديني وكل شرائع الله السماوية (اليهودية، والمسيحية، الإسلام) داعية للسلم وصلاح المجتمع. وأن جنوح الانسان للفعل المخالف لفطرته وشريعته لسبب من الأسباب يقابله الإنذار والتشديد، أو تهديد بالعقاب أو العذاب الذي يصيب من أ جرم. ولقد سمى الله سبحانه تعالى الذي يحيد عن الحق ويفعل السّيئات ويعثو فسادا في الأرض بالمجرم والمجرمين.

2 -الجريمة الالكترونية: وهي "أي سلوك غير مشروع يرتكب باستخدام التقنيات التكنولوجية الحديثة، ينتج عنه ممارسة ضغوط وتهديد وابتزاز للمجني "(الرشيدي، د.ت.، ص.35). وتعرف كذلك بأنها " ممارسات توقع ضد فرد أو جماعة مع توفر باعث إجرامي بهدف إلحاق الأذى لسمعة الضحية أو الضرر النفسي والبدني به سواء بأسلوب مباشر أو غير مباشر بالاستعانة بشبكات الاتصال الحديثة كالأنترنت وما تتبعها من أدوات كالبريد الإلكتروني وغرف المحادثة والهواتف المحمولة وما تتبعها من أدوات كرسائل الوسائط المتعددة" (https//mraitvlogs.com) ، (وعرفها المشرع الجزائري بموجب قانون 04\05 المعدل و المتمم لقانون العقوبات والمتعلق بالحماية الجزائية للمعلومات في قوله أن الجريمة هي" الدخول و البقاء غير المشروع في نظام المعالجة الآلية للمعطيات(عليوة، 2021، ص. 210)

معنى ذلك أن الولوج لنظام المعالجة بغير صفة مشروعة، ودون صفة قانونية والبقاء ضمن آلية نظام شبكة الحاسب الموصولة بشبكة النظام تعتبر جريمة معلوماتية. قد تسبب أو تؤدي إلى (السرقة أو التجسس الإلكتروني)، أو إتلاف معلومات أساسية، أو أضرار وخسائر كبيرة. وعرفها كذلك الفقيه فان دير هلست وونيف أن " هناك غياب للتعريف عام وإطار نظري متسق في حقل الجريمة...تستخدم مصطلحات الافتراضية والحاسوب والإلكترونية وكلها تعكس فجوات مهمة في التعريف". (رحموني، 2018، ص.435). وهذا يحيلنا أنه لا يوجد تعريف صريح للجريمة الإلكترونية متفق عليه أو متعارف عليه يفضي لإعطاء مفهوم صريح للجريمة الإلكترونية له دلالته الأكاديمية التي

تنبثق منه أبعاد و مؤشرات تأسس للطرح النظري والأمبريقي لمفهوم الجريمة العولمة ووسائطها ذات الابعاد الافتراضية. والذي يحتاج إلى نوع من الصقل والمرونة لفهم ماهية الجريمة الإلكترونية. (الأداة الإلكترونية والوسائط المستعملة فيها)، ويعرفها سالم وهجيج أيضا بأنها " مجموعة من الأفعال المرتبطة بالمعلوماتية التي يمكن أن تكون جديرة بالعقاب"(علي، وعبيد،2007، ص. 87). وقال عنها كذلك الفقيه الألماني تاديمان بأنها " كل أشكال السلوك غير المشرع أو الضار بالمجتمع والذي يرتكب باستخدام الحاسب الآلي" **(حوحو، وبلورغي ،2014، ص.40).** وهناك من عرفها بأنها " كل جريمة تتم في محيط أجهزة الكميوتر أو هي " كل سلوك إجرامي يتم بمساعدة الكمبيوتر "(إبراهيم، 2008، ص. 42). ويشار إليها أيضا بأنها " كل فعل أو امتناع عمدي ينشأ عن الاستخدام غير المشروع لتقنية المعلوماتية ويهدف إلى الاعتداء على الأموال المادية أو المعنوية"(الشكري،2008، ص.113).

وعليه وبناء على ما سبق نقول أن لجريمة الالكترونية إجرائيا هي الجريمة التي ترتكب في البيئة الالكترونية أو الافتراضية عن طريق نظام الحاسوب أو شبكة الحاسوب، أو الهاتف الذكي أو منصات التواصل الاجتماعي، وتسبب خطرا وخسائر مادية ومعنوية على الأفراد ومؤسسات المجتمع.

3 - **المجرم الالكتروني:** وهو المجرم الذي يستخدم الحاسوب وأي تقنية إلكترونية في نظامها الرقمي (الفعل المنحرف) لممارسة الفعل الخارج عن القانون ومعايير المجتمع، وذلك بإلحاق الضرر والأذية بالآخرين.

ثانيا -خصائص الجريمة الالكترونية:

الجريمة الالكترونية لها خصائص كثيرة تجعل عملية الاحاطة بها صعبة، ومن ثم محاربتها وصدها أمر في غاية الصعوبة والتعقيد، مما يستدعي حالة من الاستنفار الأمني من أجل الأخذ بزمام التكنولوجية وآلياتها المستخدمة في الجريمة الالكتروني. وأهم الخصائص ما يلي:

1- **تعدد أنماط المجرمين** في الجريمة الالكترونية: منهم المتسللون (الهاكارز) وهم فئة من المجرمين على مستوى عالي من الاحترافية في مجال الإعلام والحاسب. إذ يستغلون خبراتهم وقدراتهم العقلية والمهارتية للتسلل إلى مواقع إلكترونية معينة، ويمكن أن ندرج بغية الحصول على معلومات سرية أو تخريب مخزون المعلومات مؤسسة أو هيئة او حساب شخصي للأفراد، وتكبيل الضحية خسائر ضخمة. وهناك أنواع كثرة من المجرمين نذكر منهم الكراكرز أو المخترقون وعادة ما يكونوا من المحترفين أو الهواة.

2- **سهولة إخفاء أدلة وآثار الجريمة:** يرجع ذلك إلى قدرة المجرم الإلكتروني العالية في التحكم في تقنيات الحاسوب الآلي، وإخفاء آثار الجريمة، وعملية التشفير والترميز المخزن في الوسائط الإلكترونية الممغنطة ومن ثم مسح الآثار مباشرة بعد الانتهاء من العملية الإجرامية. مما يصعب من ايجاد دليل لإدانة مرتكبها وعادة ما يكتشف وجودها (الجريمة الالكترونية) بالصدفة أو بعد عدة أيام من وقوعها.

3- **النعومة**: وهذا الجانب الذي يميز الجريمة الالكترونية عن الجريمة التقليدية التي تعتمد على الخشونة والعنف المادي والقوة الجسدية (الاعتداء ، القتل)، فحين الجريمة الإلكترونية تتسم بالهدوء والنشاط العقلي المتمركز على الهدف المقصود من الجريمة دون الحاجة إلى العنف المادي أو الجسدي . إن الاحترافية والعبقرية في معالجة المعطيات والقدرة على فك التشفير والرموز الآلية للحاسوب المقترن بالشبكة المعلومات كفيلة لإتمام

الجريمة بهدوء ناعم ودون استشعار الضحية، والمجرم الإلكتروني في جهاز الحاسب هو شخص يبدو طبيعي، مسالم ولكن له شغف زائد على الجهاز بغرض التسلية والعبث أو الابتزاز أو لإظهار قدراته وقوته العقلية في اختراق البرامج (سواء ضد الأجهزة الحكومية أو المنظمات) أو لإبراز تفوقه على الحاسب الآلي(الكمبيوتر). (الفتاح، 2007، ص.46)

4- **جريمة متعددة الحدود**: أي هي جريمة عابرة للزمان والمكان، وقد تكون عابرة للحدود الإقليمية والدولية وأن الجريمة الإلكترونية في ظل الإعلام المعولم يختزل الزمان والمكان (الإجرام المنظم)، أي حدوث الجريمة في أكثر من نقطة إلكترونية مترامية جغرافيا في آنية زمنية واحد ة.

5- **العالمية** : باعتبار أن الجريمة الإلكترونية تتميز بتعدد الآنية الزمنية و المكانية فهي إحدى نواتج وسائل الإعلام المعولم الذي أنتجه التطور المتسارع للوسائل تكنولوجية الإعلام (القرية الكونية)، ولا حدود للزمان والمكان ومن ثم الجرائم الإلكترونية هي جرائم عالمية قد تكون محلية موزعة على أكثر من نقطة جغرافيا، ومنفذ الجريمة في بلد آخر (الجريمة العابرة للحدود)، كشبكة العصابات الدولية أو منظمات إرهابية دولية، وظيفتها الإجرام والتهديد والاستلاب الإلكتروني للأموال من خلال تقنيات النظام الحاسب الآلي وشبكة الأنترنت.

6 - **عدم التبليغ**: على الجريمة أو الخسائر والأضرار التي لحقت بالمؤسسة أو الهيئة أو المنظمة (سواء كانت حكومية أو أفـــــراد). كان ذلك محفزا ودافعا لتنامي الجريمة الإلكترونية وتطور أساليها وتوسع نشاطها. حيث أن تستر الشركات الكبرى والمنظمات ذات الأسهم العالمية والبنوك راجعا للخوف من فقدان الزبائن والعملاء وكذلك الخوف من تلوث السمعة وفقدان عقود عمل أو صفقات مع العملاء أو مؤسسات مالية أو خدماتية أخرى. (المكانة التنافسية بين الشركات الأخرى).

7 - **صعوبة الكشف عنها و اثباتها** : تتميز الجريمة الالكترونية بصعوبة اكتشافها وهذا راجع للقدرة المجرم الإلكتروني على التخفي ،و إخفاء أداة الجريمة و آثارها .حيث لا يتم اكتشاف وجود جريمة على الضحية ما إلا بمرور وقت طويل عليها أو عن طريق الصدفة . وذلك لقدرة المجرم على مسح أو "تدمير دليل الجريمة في أقل من الثانية الواحدة «(براهيم، 2016، ص.213).

ثالثا – المعالجة النظرية للموضوع:

إن الحديث عن موضوع الجريمة الالكترونية أسبابها والعوامل المؤدية إليها موضوع شائك ومترابط، أفرزته عوامل كثيرة ومسببات معقدة تشترك فيه الكثير من المجتمعات، وتختلف فيه الكثير منها. لأن اشكالية الإجرام والمجرم الإلكتروني كمتغير له علاقة بتغير البنية الأنثروبولوجية للإنسان المجرم والبيئة الإيكولوجية الفعلية والافتراضية، والوسيلة التقنية المعولمة. هذه الثلاثية الأبعاد التي تأسس لمسرح الجريمة من منظور أنثروبولوجيا القانون وأنثروبولوجيا الجريمة. والذي يفرض علينا الوقوف على أكثر من محطة للحديث عن الجريمة الإلكترونية التي لم تعد مجرد جريمة بسيطة غير منظمة، بل أضحت جريمة عالمية بأبعاد متشعبة أفرد لها الكثير من الباحثين والعلماء كل وفق تخصصه الكثير من الدراسات والأبحاث العلمية والقانونية والسوسيو أنثروبولوجية والنفسية . وذلك للإحاطة بالظاهرة المستحدثة وتبيان أسبابها وخصائصها، وأنواعها وآثارها على الأفراد والمجتمع من أجل الحد من خطورتها وتداعياتها (انعكاساتها). وسنحا ول إبراز أسباب الجريمة الإلكترونية وتبيان العوامل المساعدة على

ذلك، مع ذكر بعض أنواع الجريمة الإلكترونية بغية استدراج بطريقة تحليلية واستنباطية لبعض العوامل والأسباب التي تكون لها دخل بطريقة أو أخرى في الجريمة الإلكترونية.

أولا -أسباب الجريمة الالكترونية:

إن ظهور أي ظاهرة في المجتمع سواء كانت إيجابية أو سلبية، محلية أو عالمية لها أسبابها التي تعطي مبررات ومؤشرات في كنه الظاهرة "الجريمة الالكتروني" بأبعادها السياسية والاجتماعية والنفسية والاقتصادية والثقافية. ومن جهة أخرى أن مسرح الجريمة ومستوى الفعل الاجرامي يختلف أسبابه باختلاف الأفراد وفئاتهم واختلاف الأهداف والنظام التخطيطي المعد للجريمة، وكذلك اختلاف نوع الضحية.

سنحاول ذكر بعض أسباب الجريمة الإلكترونية بأبعاد مخصوصة:

1.1الأسباب النفسية:

1.1 -الدوافع الداخلية (الذاتية): الفضول وحب الإثارة والمغامرة والتحدي اتجاه الوسيلة التكنولوجية (الحاسوب أو نظام شبكة الحاسب الآلي أو اتجاه التطبيقات والوسائط الإلكترونية). وهي سمات الشباب والمراهقين. حيث يكون هناك نوع من التفاعلية الرمزية و الرقمية بين شغف الفرد وحالته الكميو نفسية، من منظور الوضعية و الاتجاه النفسي في الأنثروبولوجية التي تنظر بمنظور تكويني و نفسي، فشغف الشخص والاستمتاع بالجرم تضعه في خانة الجنون (المجرم المجنون) .وامتداد ذلك في عصر التكنولوجية المعولمة والهوس نحو شبكة المعلوماتية ونظام الحاسب الآلي، يجعل هذه المقاربة النظرية تشكل بعد سيميولوجي تكويني وشخصي اتجاه فعل الجريمة ضمن مجالها الإلكتروني المغنط والسالب للذات المهوسة بالتقنية وذوي المهارات العالية والأذكياء، الذين لهم القدرة على الاحتفاظ بالصور والأفكار و الأحاسيس وتخزينها وتجمعيها ثم تحليلها (نيص، الزهيري، 2017، ص. 89) وللاستعانة بها بعد ذلك لممارسة فعل الجريمة. تستفز التقنية ذاتية الفرد نحو إثارة جملة من التحديات والفضول نحو نقاط معينة من نظام المعلوماتية أو الوسائط الإلكترونية في مواقع محدودة. تتبعها أفعال وسلوكيات خارج عن الذات المجازفة، وذلك للوصول إلى الهدف المسطر. وعادة ما يكون المجرم في هذا المستوى من فئة الشباب الهاوي أو المحترف، أو من نفس نهج الجريمة الإلكترونية. يعبر القراصنة أن عملية القرصنة والعبث على الحاسوب والشغف به يصاحبه النشوة والمتعة في ممارستها كهواية وتسلية. حينها تعطي نشوة التحدي والمخاطرة والصراع الداخلي الذي يصاحبه تفاعلات متداخلة نفسية كيميائية فالمجرم "يستخدم مقدرته العقلية ..ليحقق أهدافه بهدوء"(المومني،2008، ص.77) . في القرصنة على النظام الذي يعتبره، وكأنه لعبة يلهو بها الاطفال"(بحري، وخرموش ،2021، ص.51)، لذا نعتقد أن أهم الدوافع السيكولوجية تكون وراء قيام الجريمة الالكترونية (الإثارة وما يتبعها من متعة). تفضي إلى نوع من التفاعلية الرمزية بين الذات والوجدان والوسيلة الالكترونية المستعملة. وهي عملية معقدة تعتبر أحد العوامل والأسباب لارتكاب الجريمة الالكترونية على الحاسوب.

1.1 - البحث عن الثراء والربح السريع (الدافع المادي): بحكم التغيرات الاجتماعية و التقلبات الاقتصادية التي يعيشها الفرد في مجتمعه. على اعتبار أن الشخص لا يعيش بمفرده بل في تفاعلية ديناميكية مادية مع الآخرين. وفي ظل اكتساح العولمة الثقافية وسيطرة الاعلام المعولم، تغيرت الثقافة الاستهلاكية للأفراد وتبدلت المفاهيم والقيم

التي تشكل ثقافة المجتمع ومؤسساته. أين أصبح الدافع المادي هو الحصول على المال والثروة بأي شكل كان. مما جعل الجنوح للجريمة الإلكترونية (كالنصب والاحتيال الإلكتروني، والابتزاز، القرصنة، الإرهاب الإلكتروني، طلب الفدية) هو الدافع والمحرك النفسي الأساسي لارتكابها. وذلك طمعا في المال وتكوين الثروة (بوسائل غير شرعية). واللهفة على كسب المال والثروة في فترة وجيزة أو قصيرة، نابعة من الذات المرضية التي تستتر على كل فعل إجرامي باستعمال التكنولوجية المعولمة. حيث "أشارت مجلة (Securite infom antique)أن 43 % من الغش المعلن عنها كانت من أجل اختلاس أموال و 23 % من أجل سرقة معلومات، و 15% سرقة وقت الآلة و 19% أفعال اتلاف"(المومني، 2008 ، ص. 90).

1.3 - الرغبة في التسلية والدافع للبحث عنها : حين تكون الرغبة في البحث عن التسلية من الرغبات النفسية التي تحتكم إليها النفس البشرية من منظور الانثروبولوجيا النفسية والاجتماعية، والجنائية التي تتعمق في الآنية الشخصية للإنسان المجرم الإلكتروني و بنية الشخصية الجانحة في ظل تشكلها ملامح الأنا بمراتبه الثلاثة، ومدى انعكاس ذلك على السلوك الفعلي للفرد. فالميل للترفيه والتسلية يتوقف على الصفة الأنثروبولوجيا لتركيبة النفس السوية أو حتى العابثة. ومكونات البيئة الإيكولوجية والافتراضية التي توفر فرص الترفيه والتسلية.

ومن ثم أن الانحراف والجنوح السلوكي في ظل الحاسب الآلي أو شبكة الحاسب الآلي والتسلية، تجعل الفرد يقع في الجريمة الإلكترونية بطريقة أو بأخرى بفعل التسلية على حساب الآخر، وإيذاء الاخر (الولوج إلى حساب أشخاص والعبث بالمعلومات الخاصة أو إتلافها أو إخفائها أو سرقتها). بطريقة مقصودة أو غير مقصودة مع الاستمرارية يتحول الشخص الهاوي إلى مجرم محترف في حدود المجال الذي يختص به. ويكون الغرض من ذلك إما تعطيل نظام الحاسب أو تدمير بيانات وتعطيل مصالح الاخرين .

1.4 -دافع الانتقام (الرغبة في الانتقام): قد يكون الانتقام هو الدافع المحفز للارتكاب الجريمة الإلكترونية. حيث يكون الداع للانتقام موجها نحو فرد بعينه أو جماعة ما أو نحو هيئة أو مدير عمل أو مسير شركة التي يعمل فيها أو اتجاه مالك الشركة أو اتجاه أنظمة مؤسساتية سياسية. وذلك إما بتخريب قاعدة المعطيات أو ادخال فيروس في الحاسوب الآلي يعمل على تخريب المعلومات والبيانات أو يعمل على سرقة المعلومات واعطائها لشريك آخر رغبة في الانتقام.

1.5- الاضطراب النفسي : قد يرجع إلى خلل في شخصية الفرد أو مرض نفسي ، يجعل الفرد يستعمل السلوك الضار والعدواني و العنف الالكتروني، في ظل الأنتروبولوجية التكنولوجية التي صنعت كينونة و بنية الانسان المعاصر. وعليه الادمان على شبكة الحاسوب أو نظام الحاسوب أو شبكة الهاتف الذكي ينعكس سلبا على نفسية المدمن (الاحباط والاكتئاب والاضطراب النفسي) قد تكونا سببا للاضطراب النفسي الذي قد تؤدي إلى فعل الجريمة وممارسة العنف الرمزي أو الالكتروني الذي يتسبب في تدمير قاعدة البيانات الشخصية لأشخاص ما أو التلاعب ببيانات النظام الآلي للحاسب .

1.6 - الذات المنخفضة : إن وجود مثل هذه الذات له بواعث نفسية وعوامل أخرى معقدة تعمل على تكبيل الذات و طمس إحدى معالم الايجابية، وبروز السلبية الإلكترونية في التعاطي مع الأداة التقنية كفيل بممارسة

السلوك السلبي والاستغلال المادي والجنسي في المواقع والوسائط الالكتروني التي تكون إحدى أسباب تبلور وتشكل الجريمة الالكترونية.

2-العوامل والأسباب الخارجية:

الأسباب والعوامل الخارجية هي كل العوامل الخارجة عن الذات وكينونة الفرد. حيث تعمل كقوة ضاغطة تدفع الفرد إلى فعل الجريمة الالكترونية أو ممارستها كنشاط مادي، أو داعمة لنشوء الجريمة الالكترونية ومن ثم ارتكابها. بتواطؤ جهات معينة بطريقة أو بأخرى.

2.1 -الأسباب الاجتماعية: تتدخل العوامل الاجتماعية في نشوء الجريمة الالكترونية، حيث يعمد المجرم الإلكتروني على اختراق الحاسب الشخصي أو الأجهزة الإلكترونية الخاصة بشخصية بعينها. بغية التعرف على نقاط ضعف شخص ما أو الإساءة لأحد أصول الأسرة وتاريخها ومكانتها، أو بدافع الاستلاب المادي والمساوة المادية أو الانتقام .... إلخ.

2.1.1 -الأسرة والاجرام: الأسرة هي المؤسسة الاجتماعية والبيئة الأولى التي تتكفل في انتاج الأفراد وقولبتهم وفق مناهج وأساليب تربوية مختلف فيها، حيث يتشكل ويتركب الكائن الإنساني وتتبلور فيه إنسانيته وتحدد فيه معالم كينونته، وشخصيته ووجدانه وتفاعلاته. والأسرة هي الحاضنة المسؤولة عن تنشئة الأفراد نفسيا وتربويا وروحيا وفكريا، وعقليا، اجتماعيا. وهي التي تزوّد المجتمع بأفراد صالحين أو جانحين. باعتبار أن البناء الأنثروبولوجي للشخصية الحدث يتطلب التكاملية بين عناصر البناء، فأي تقصير أو تخاذل في وظيفة الأسرة الأساسية (التنشئة الاجتماعية الصحيحة) تؤذي إلى اضطراب في الشخصية والسلوك والذي يترجم تمرد الكائن الانساني الصغير على قيم الأولياء. وعادة ما يؤدي إلى الانحراف والجريمة. يقول الله تعالى في سورة التحريم "يـاَ أيّهاَ الـذينَ ءَامَنُوا قُوا أَنْفُسَكُمْ وَأَهَالِيكُمْ نَاراً وَقوُدُهاَ النَّاسُ وَالحِجَارَةُ عَلَيهاَ مَلاَئِكَةٌ غِلاظٌ شِدَادٌ لاَ يَعْصُونَ اللهَ مَا أَمَرَهُمْ وَيَفْعَلُونَ مَا يُومَرُون " (القرآن الكريم: سورة التحريم، الآية 6). الآية الكريمة واضحة تدعو إلى ضرورة اهتمام الأسرة بأفرادها وتربيتهم وتنشئتهم تنشئة صالحة وفقا لقيم المعتقد والثقافة المجتمع التي تدعم استقرار الأفراد والأسرة ومن ثم صالح الفرد هو صلاح للمجتمع. حيث توكد العديد من الدراسات التي أقامت على المجتمعات الإسلامية أن ما يحدث في الأسرة من مشكلات وخلافات وصراعات بين الأزواج أو بين الأبناء والوالدين، والأساليب التربوية (المعاملات) مع الأبناء، وطبيعة ونوع العلاقات السائدة بين أفراد الأسرة الواحدة في ظل تغلغل الوسائل التكنولوجية الحديثة داخل كنه الكائن الأنثروبولوجي (الأسرة). فرض نوع من عدم الانسجام والاغتراب النفسي والاجتماعي على مكونات البنية العلائقية للأسرة. والذي كان دافعا وداعما لجنوح الحدث أو أحد جزيئيات البناء الثقافي الجديد المنتقى، والمحررة للقيم الايجابية والسلبية. وذلك حسب طبيعة التشكيلة الاجتماعية والثقافية للبناء الأسري. أي أن سلوك الجانح والولوج إلى الإجرام المعلوماتي (الإلكتروني) له صلة وثيقة بما يحدث داخل الأسرة.

2.1.2 - من جهة أخرى التغير الاجتماعي في ظل العولمة الكاسحة لثقافة المجتمع ، لها انعكاسا سلبيا على مقومات الأسرة ووظيفتها . إذ فرضت الضغوطات الخارجية خروج المرأة للعمل، وهذا الأخير خلق شرخا في التنشئة التربوية والوجدانية والنفسية للأحداث الصغار. إذ أن غياب الأم عن المنزل لفترة طويلة ينعكس سلبا على تنشئتهم. يستفزنا

التساؤل هنا إلى من يترك الطفل أو الحدث؟ هل تستطيع الوسائل التكنولوجية الحديثة والمواقع الإلكترونية والتواصلية الموجودة على الهواتف النقالة أو اللوحات الرقمية، أو الحاسوب أن تقوم بإحدى وظائف الأسرة؟ من يراقب الطفل في غياب الأوين؟ ما هي الأشياء التي يشاهدها المراهق وتجذبه؟ مع من يتواصل الحدث؟... أسئلة كثيرة توردنا لا نستطيع الاجابة عليها آنيا.

وعليه نقول إن غياب المرأة عن البيت لفترة طويلة مع غياب الأب كذلك للعمل، مع وجود وسائل التواصل الاجتماعي تجعل النظرة الأنثروبولوجيا والتحليل الديناميكي لهذه العلاقة الثلاثية وتشكلها وتبلوها هو تأسيس لمسار الحالة وتاريخها قبل وبعد تتشكل الفعل "الإجرام الإلكتروني". وأن عامل التغير الاجتماعي فتح منافذ التفكير الاغترابي الشذوذ النفسي، والوجداني وضعف الاتصال العائلي. وأغلب الدراسات تؤكد أن الجنوح (الحدث أو الشاب) له صلة وثيقة بالمحيط الأسري والتغير الاجتماعي الحاصل في المجتمع. وأن تخلي مؤسسات المجتمع بما فيه الأسرة على إحدى وظائفه أورث المجتمع الكثير من المشكلات. والمتعارف عليه قديما وحديثا أن الأسرة ككائن أنثروبولوجي هو الذي ينمذج تفكير وقيم جزيئات بنائه، (المخرجات)، وهو الذي يقولب السلوك وفق ثقافة المجتمع التي تصطبغ كينونة الحدث الانساني. كبناء يحتاج إلى ترويض وتأهيل في خضم الضغوطات الخارجية الممارسة على الأسرة. كل هذه المؤشرات تعتبر سببا لنشوء الجريمة الإلكترونية وانتشارها.

2.1.3 -البعد الأخلاقي والاجتماعي (الوازع الديني): قد يكون السبب في الجريمة ذا بعد أخلاقي إذ يعمد الشخص من خلال حسابات مزورة أو من خلال فضاءات إعلامية، بنشر دعايات واشاعات مزيفة وكاذبة من أجل تشويه اسم عائلة لها تاريخها المشرف أو شخصية مرموقة في المجتمع، أو من أجل الانتقام أو تصفية حسابات، ومن جهة أخرى قد يتخذ البعد مسلك آخر إذ يعمد المجرم الالكتروني أو شخص ما إلى كشف أسرار شخصية لشخص ما له مكانة اجتماعية أو اقتصادية على وسائل التواصل الاجتماعي أو وسائل الإعلامية أخرى كداعية مغرضة (من أجل الانتقام أو المساومة، أو ...) حيث أن تسريب بعض المعلومات الحساسة قد تفضح صاحب الحساب وتشوّه صورته أو تكشف نقاط ضعف عائلة بعينها . لتنتقل الأخبار والمعلومات إلى البيئة الواقعية، ويكون ذلك إحدى المؤشرات الاجتماعية لنشوء الجريمة الالكترونية (الابتزاز الالكتروني، والمساوة المادية أو المالية). (المايل، الشربجي، وقابوسة، 2019، ص. 248).

2.1.4 - **التعلم والمحاكات:** تعلم مهارات نظام الحاسب الآلي يكون حافزا أكثر للتواصل و الاحتكاك عبر منصات التواصل الاجتماعي أو الشبكات المعلوماتية ، التي تعطي للفرد الانساني نوعا من الاستقلالية والاستباحة للولوج إلى مواقع تعليم واكتساب الخبرات على يد مختصين. وبالتالي عملية التعلم كسيرورة سيوسيو أنثروبولوجية تقتضى نوع من التفاعلية للاكتساب التعلم، والذي يكون بدوره دافعا للإجرام الإلكتروني، من خلال تقصي حواسب أخرى وقرصنتها بطريقة مقصودة أو عفوية في بدايتها. لذا يكون التعلم الفردي أو الاجتماعي في البيئة الافتراضية مقترن بنقاط إلكترونية يشرف عليها مجرمون محترفون أو مختصون يروجون إلى نوع معين من البرامج، قد تكون سببا لتعلم المبادئ الأولية للإجرام، أو تعلم أساليب جديدة للإجرام الإلكتروني أو الانخراط في عصابات إجرامية إلكترونية. مما يؤدي إلى نوع من الاحترافية في مجال معين من الإجرام الإلكتروني. وقد يؤدي إلى توسع رقعة الجريمة الإلكترونية وتعدد وسائطها. ولو تتبعنا خريطة تعلم الإجرام لأوردنا ذلك إلى المقاربة النظرية للأنثروبولوجي لـــ دوين سذرلاند

eduin sutherland في نظرته التي فسرت كيف يمكن أن يتعلم الانسان أو الحدث الاجرام؟ وأرجع ذلك إلى التعلم الاجتماعي والتقليد والمحاكاة. (عن طريق التفاعل والاحتكاك المباشر أو دونه بالمجرمين على اختلاف جرائمهم). أين يتم انتقال الخبرات والقيم والمبادئ التي تؤسس للجريمة، وتبرر الفعل والسلوك الإجرامي. والترابط التفاضلي من منظور سذرلاند قائم في المجتمع الإنساني، حيث يعكس مفاهيم كثيرة. وأن الصراع الثقافي والتنظيم الاجتماعي والتفاضل الفارقي الموجدان في المجتمع يعطي أبعاد سوسيو أنثروبولوجية في تفسير ظاهرة الاجرام وعملية التعلم الاجتماعي والجماعي للفعل الذي يتضمن تفسيرا ت للجريمة. (Marilyn , 2013 , P. 117) . ولو أسقطنا هذه النظرية في ظل وسائل العولمة ومواقع الالكترونية في وقتنا المعاصر، يكون للفضاء الافتراضي وما يبثه من ثقافة غربية مشبعة بقيم تعزز لقيم الاغتراب والابتعاد عن المعتقد في نقاط إلكترونية مفعلة من مختصين وناشطين من جنسيات مختلفة. تعمل على ترويج مضامين ثقافية جانحة وفق برامج تعليمية سواء لآليات النظام وشبكة الحاسب الالي، أو في مجال التقنين لمهارات وخبرات لتعليم أصول الجريمة الإلكترونية بأشكالها وفق قوالب مقفلة برموز. تسهل الانخراط في شبكة إجرامية، أو صناعة الإجرام إن صح التعبير. وعليه فالرغبة في التعلم أو التعلم الاجتماعي كانت نقطة ارتكاز حيوية للتحريض على تفعيل الفعل الإجرامي المعولم. أي أن تعلم الأنماط الإجرامية في الوقت الحالي وفي مجتمعاتنا المعاصرة وفي ظل وسائل التواصل الاجتماعي سهل تعلم الجريمة الإلكترونية من بابها الواسع.

2.2 - **الضغوط العامة:** إن الضغوطات التي تمارسها التغييرات الحاصلة في الساحة العالمية و المحلية تعكس مدى التناقضات التي تفرزها على كل الأصعدة السياسية والاجتماعية والاقتصادية وحتى الثقافية. تشكل كنسيج سوسيو أنثروبولوجي لحركية مسار المجتمعات والتقاطعات الحادثة على مر التاريخ الذي يصور استمرارية تدفق الأنساق في سلسلة تعكس تطور فكر الإنسان البشري، وتطور ابتكاراته العقلية والابداعية... إلى صناعة التكنولوجية والحضارة. وما أفرزته من إيجابيات وسلبيات على الأفراد والمجتمعات. سواء المتقدمة أو دون ذلك. إذ تؤدي التحولات والتغييرات الحاصلة في المجتمعات إلى تشكل الأعباء والضغوطات العامة على الافراد التي قد تقفل منافذ السلم والرزق والراحة على الانسان (مشكلات، وصعوبات مالية، ومادية، ظروف العمل، أو انعدامه، ضعف الدخل الفردي، الوضعية الصحية للأفراد الأسرة أو العائلة، الوضعية الوبائية لفيروس كورونا مثلا ما انجر عنها، نكسات وصعوبات نفسية واجتماعية واقتصادية ...إلخ) كل هذه الصعوبة والضغوطات أثرت سلبا على المسار السلوكي للأفراد. إذ أدت إلى زيادة معدلات الجريمة الإلكترونية على اختلافها في الكثير من الدول، ومن جهة أخرى قد تساهم بطريقة أو أخرى في صناعة الإجرام الإلكتروني والمجرم الإلكتروني. كما فتحت أفق لكسب المال والموارد المادية (كسب ضروريات العيش خاصة الحياة في المدن الكبرى)، وكما كانت منفذا للهروب من الضغوطات والظروف القاسية والولوج إلى عالم الجنوح والاجرام .(البداينة، 2014، ص.14).

2.2.1- **البطالة**: عدم توفر مناصب عمل وعدم وجود مداخل مادية أخرى قد تكون سببا كافيا لارتكاب الفعل الإجرامي. وأن انتشار الجريمة الالكترونية بين فئات المجتمع الواحد على اختلاف ثقافته يخلق نوع من لا توازن في المجتمع. ومع التغييرات التي يشهدها المجتمع الجزائري أو المجتمعات العربية على جميع الأصعدة أدى إلى نوع من التشابك والصدام بين ثقافتين مختلفتين، تستند كل منها إلى إطار قيمي. ومن جهة أخرى قساوة الظروف الاجتماعية وتفاقم المشكلات الاقتصادية، قابلها انسداد في سوق العمل، وتسريح الكثير من العمال. مما أدى إلى ارتفاع معدلات البطالة بين كل الفئات الشابة، وعلى اختلاف مستوياتها وخبراتها التكوينية والتحصيلية. وعليه البطالة كواقع يعيشه

الكثير من أفراد المجتمع الجزائري تقف حجرة عثرة أمام طاقات وكفاءات عالية في شتى التخصصات العلمية والتكنولوجية قد تقدم الكثير لمجتمعاتها. إلا أن ضعف تأطيرها وعدم استغلالها (غلق سبل النجاح والعمل) ينعكس سلبا على توجهاتها. وقد تجنح إلى عالم الجريمة الإلكترونية من أبوابها الواسعة وتكون بذلك أكثر خطرا وضررا على المجتمع (كلام نسبي). أو قد تمتهنها كوسيط إلكتروني أو كمنفذ لاستقصاء عملاء أو ضحايا. أو ... إلخ. (مخدرات إلكترونية، ابتزاز أو انتحال الالكتروني.

2.2.2 -مستوى التحضر: أمام تزايد تدفقات الهجرات الداخلية والخارجية من وإلى المدن الكبرى، شكلت هذه الأخيرة ضغطا كبيرا على مدن بعينها. فيما يخص توفير متطلبات الحياة والتأقلم مع البيئة الجديدة، وتغيير نمط العيش والسلوك، عدم وجود مأوى. مما يتطلب نوع التكيف والتوافق مع الظروف البيئية الجديدة. ولو نظرنا بمنظور أنثروبولوجيا المدينة التي تصور لنا ثقافية المدينة أو العمران البشري وتشكلاته الاجتماعية والثقافية التي تصطبغ وتتجلى في تصرفات ومعاملات وسلوك الأفراد، وعمران المدينة وطبيعته المعمارية تعطي للأنثروبولوجية الحضرية تصوير شخصية الثقافة المعمارية والحضرية لإنسان المدينة، وبالتالي الهجرة الداخلية المحلية من وإلى أو الخارجية وإلى المدن الكبرى (دخول تشكيلة اجتماعية وثقافة مختلفة ،وطبائع مختلفة) تفرض على النازح أو المهاجر جملة من العوامل(التكيف والتوافق والعمل). لتحقيق أسباب البقاء والعيش في المجتمع الجديدة. وعليه تكشف طبيعة الثقافة البيئية لأنثروبولوجيا الحضرية والأنثروبولوجيا الاجتماعية تأثر سلوك الأفراد سلبا أو إيجابا لما هو قائم بالفعل، أين يلجأ الكثير منهم إلى أساليب جانحة من أجل توفير مستوى معين من التحضر الاجتماعي والمادي. حيث وفرت التكنولوجية الجديدة أساليب كثيرة لتعلم الاندماج الإلكتروني في البيئة الافتراضية. أين يطرق الكثير من الأشخاص النازحين أو المهاجرين عالم الجريمة الرقمية كوسيلة لتوفير المال وتخفيف ظروف المعيشة، والتكيف الاجتماعي. وتكشف الأنثروبولوجيا الجريمة أن عملية تشكل السلوك الإجرامي أسبابه عادة تؤول إلى عدم التوافق الاجتماعي والايكولوج. الذي يفسر طبيعة الشخصية للإنسان المجرم وبنيته المورفولوجية والنفسية. حينها تكون عوامل المدينة ومستوى التحضر كأسباب داعمة لولوج المهاجر إلى عالم الاجرام والجريمة سواء التقليدية أو الإلكترونية.

2.3 -العولمة: إن التدفق المتسارع للمعلومات واكتساح ثقافة العولمة كل المجتمعات العربية والإسلامية وظهور الفضاء الافتراضي أو الإلكتروني، عزز وساعد على تشكل العلاقات الافتراضية، والصدقات المتعددة مع الأجناس. وكذلك نوعية ومضمون الرسائل الثقافية والإعلامية التي تبثها وسائل الإعلام الجديد ومواقع التواصل الاجتماعي التي تؤسس ضمن برامج تعليمية وتوجيهات رقمية. في كيفية استعمال النظام الرقمي وأنظمة الإعلام الآلي التي قد تكون أحد أسباب انتشار الجريمة الإلكترونية، وصناعة المجرم الإلكتروني على المستوى المحلي والدولي.

2.3.1 - الارهاب الاعلامي ودوافعه: يعتبر التهديد الارهابي الذي يمارس في الفضاء الافتراضي اتجاه دول ما ، أو داخل إقليم معين جريمة إلكترونية. يسعى من خلاله الإعلام المعولم لإشعال الفتنة الطائفية أو العقائدية بين أفراد المجتمع الواحد، ويعمل كذلك على تلويث الأخبار و تضخيم الأحداث وتشويهها، وبث الفرقة بين الشعوب (بين دولتين متنازعتين). مما يؤجج التوترات والنزاعات في المنطقة، وينعكس سلبا على استقرار المجتمع ومنطقة النزاع. وقد يتسبب في المساس بالأمن الداخلي للدولة. وعليه يعمد الاعلام المعولم إلى ممارسة الجريمة الإلكترونية بطريقة غير

مباشـرة فيها نوع من التحريض على العصـيان. وتأجيج الفضـاء الإجرامي الإلكتروني لدس الأخبار الكاذبة والتخويف والتهويل. لأجل تكبيل عمل الحكومات، وتشتيت مساعيها في السيطرة على الأمن الداخلي ودفع عجلة التنمية والتطور. ومن ثمّ خلق الحروب السـيكولوجية المبرمجة في الإعلام المعولم هو "الحرب الإلكترونية" من أجل صـناعة صـورة ذهنية سلبية عن مشاكل الشعب وسلبية الحكومات، التي تعزز لظهور الثورات الشعبية ضد الحكومات كما حصل في الكثير من الدولة. (كلام نسبي)، واستفحال الجريمة الإلكترونية بين فئات المجتمع وانتشارها.

2.4 – أ **سـباب تتعلق بخصـائص الجريمة الالكترونية**: (البداينة، 2014، ص.19). نذكر منها الإزالة مقابل الاحتفاظ والاسـتنسـاخ وهي متعلقة بآثار الجريمة وسـرعة التخلص من الأداة والآثار المترتبة عليها في أقل من سـرعة ضـوئية. وكذلك التوافر مقابل توفر الشـبكة والديمومة القيمية، مقابل بطاقات الائتمان والحسـابات المالية الأخرى والمصـرفية، وسـرعة التنفيذ مقابل لمسـة وضـغط على زر الحاسـب الآلي تتم عملية الجريمة في أقل من لمحة زمنية ......إلخ أي لا وجو د لمسـرح الجريمة (الجريمة) الآنية والدلائل الجنائية الدالة على ذلك، وكل هذه الخصـائص قد تكون كمؤشـرات قابلة لتدوير والتدويل لتصـبح أسـباب فعالة لارتكاب الجريمة المعلوماتية بأي طريقة كانت وفي أي وقت.

3 -أنواع الجرائم الالكترونية:

تتشـعب الجريمة الالكترونية وتتنوع أشـكالها مما يصـعب بمكان تحديد أنواعها. وسـنحاول تصـنيف الجرائم كما يلي: -جرائم إلكترونية ضـد الأفراد: وهي الجرائم التي تمس الأفراد وتسـتهدف هويتهم وانتحال شـخصـيتهم، وتتم من خلال الحاسـب الآلي أو شـبكات الحسـاب الالكتروني أو الايمايل الإلكتروني، أين يتم فيها اختراق وسـرقة (القرصنة)، الحسابات الشخصية أو انتحال الشخصية أو تدمير أو اتلاف المخزون المعلوماتية من أجل الحصول على المال أو المعلومات السرية.

3 - 1- جريمة الابتزاز الالكتروني للأشـخاص: ويتم ذلك بواسـطة الحاسـب الآلي أو أي وسـيلة إلكترونية حيث يتم الابتزاز الإلكتروني باختراق الحسابات الشخصية وسرقت الملفات المهمة والصور والبيانات بغية ابتزاز الأفراد ماديا أو جنسيا وذلك للحصول على المال (ttps//cyberone.co).

ويكون الابتزاز الإلكتروني لأسـباب كثيرة نذكر منها: - الابتزاز لأجل الانتقام من أشـخاص معينين . - سـرقة بيانات ومعلومات خاصة بالشركات بناء على نوع الجريمة الإلكترونية " الابتزاز الإلكتروني "يحدد لنا السبب الجريمة الإلكتروني:

أ- دافع الانتقام الذي تشكل نتيجة ممارسات و معاملات شاذة. قد يكون الانتقام موجة اتجاه شخص معين أو اتجاه شـركة ما، واتجاه مدير مسـير، وقد يتعدى ذلك الانتقام ليمس نظامين مختلفين من دولة واحدة أو بين دولتين متباعدتين.

3.2 -جريمة الدعارة والاستغلال الجنسي للأطفال في الأنترنت ومواقع التواصل الاجتماعي إن نشر الصورة الاباحية في الفضـاء الرقمي من قبل مواقع مختصـة يقودها جهات مجهولة أو معلومة تسـتغل الاطفال أو الطفولة في لوحات الاشـهار للترويج للجنس والدعارة. وهذه الجريمة هي اغتصـاب لحق الطفل في العيش في مرحلته العفوية والبراءة.

فاستغلال الطفل جنسيا يفضي إلى ممارسة الجنس أو الظهور في مواقع ومواقف مخزية تجعل الطفل على المدى الطويل يتحول إلى مجرم عنيف يحتقر ذاته ويمارس سلوك الاغتصاب بكل وحشية. ومن ثم يمكننا أن نستخلص السبب أو الدافع من وراء هذه الجريمة وهو:

ب -**تجارة الجنس والدعارة:** والتي تتم على مواقع إلكترونية مخصوصة هدفها اغرائي تجاري تستغل فيها الطفولة لجذب العملاء الالكترونيين من خلال لوحات إشهارية لا أخلاقية تروج للجنس والمثلية والتي تذر علها بأموال وأرباح خيالية وهذه الأفعال قد تكون سببا لممارسة الجريمة الالكترونية بين الصغار والكبار. ويؤدي إلى تسويقها كسلعة استهلاكية إلى كل دول العالم وبخاصة الدولة الاسلامية.

- عملية التجسس الالكتروني على حكومات مما يودي ذلك إلى تهكير أنظمة الامنية للحكومات، أو سرقة معلومات سرية (القرصنة). لها علاقة بسياسة واقتصاد دولة ما. وقد يؤول هذا الدافع أو السبب إلى:

ج - دافع التنافس السياسي و الاقتصادي : والذي عادة ما يكون بين دولتين أو معسكرين وحسب نهلا عبد القادر المومني أن قراصنة من الروس قد قاموا باختراق حسابات، وسرقوا معلومات سرية وحساسة من أجهزة حواسب عسكرية تابعة لحكومة الولايات الأمريكية. (المومني، 2008، ص.39).

جرائم سياسية: تستهدف هذه الجرائم المواقع العسكرية والأنظمة الامنية والعبث فيها. أو تسريب السياسة الأمنية للدولة ما أو تدمير وتخريب الأنظمة الأمنية لها. مما يعرض أجهزة الأمن الداخلي لدولة ما إلى هجمات إرهابية وأخطار أمنية كبيرة.

د -**السباق نحو التسلح والتنافس العسكري:** حيث يحتدم الصراع والتنافس العسكري حول امتلاك زمام القوة المادية، يدفع الدول المتنافسة إلى ممارسة فعل الجريمة الإلكترونية بالقرصنة وسرقة المعلومات السرية عن السلاح والجيش والمنشآت العسكرية المادية والافتراضية.

خاتمة:

من خلال الطرح النظري لأسباب الجريمة الالكترونية تبين أن البيئة الرقمية الموصولة بالعالم الالكتروني أو الافتراضي تكون بؤر للجريمة المعلوماتية. وذلك لارتباط أنشطة وأعمال الأفراد أو المؤسسات أو المنظمات بالحاسب الآلي ونظام الشبكات الالكترونية. من جهة أخرى أن أغلب المعلومات ومخزون الوثائق والسندات المالية والرقمية، أو حتى وثائق المعلومات السرية، مخزنة في المخزون الإلكتروني. وأن القراءة السوسيو أنثروبولوجي لأسباب الجريمة الإلكترونية واقتراف الفعل الاجرامي، يرجع لأسباب ودوافع مختلفة لها امتدادها القديم في المجتمعات البدائية وتطور الانسان واختراعاته الحديثة، التي أعطت صبغة جديدة للجريمة ورسمت فضاء آخر افتراضيا يصنع من خلاله الاجرام والمجرم الإلكتروني (القدرة على التخفي، والتستر ومحو أثار الجريمة). وهذه السمات جعلت أثار الجريمة الالكترونية لا تعد ولا تحصى، سواء على الأفراد أو المجتمع.

توصيات الدراسة:

✓ ضرورة تأمين قاعدة المعطيات للحاسب وذلك باقتناء برامج وقائية عالية.

✓ توظيف مختصين وذو الكفاءات العالية في الاعلام التكنولوجي والاتصال لإدارة المصارف والإدارات المالية والمخزون المعلوماتي للمؤسسة أو المصارف الكبرى.

✓ ضرورة انشاء جهاز وقائي وافتراضي جاهز لمواجهة كل الطوارئ والاحتمالات المفاجئة المستجدات لمجابهة الاحتمال للجريمة الالكترونية.

✓ تفعيل الإعلام الموجه على صفحات الأنترنت وشبكات التواصل الاجتماعي، لترشيد وتوعية الشباب، وفتح سبل العمل والاحتكاك فيما بينهم.

قائمة المراجع:

1) القرآن الكريم

2) إبراهيم، خالد ممدوح. (2008). أمن الجريمة الإلكترونية. الإسكندرية: الدار الجامعية

3) بحري، صابر، وخرموش منى. (2021). أهم الدوافع السيكولوجية وراء الجريمة الالكترونية. مجلة دراسات في سيكولوجية الانحراف، 6(1)، 36-59

4) البداينة، موسى ذياب. (2و4 سبتمبر، 2014). الجرائم الالكترونية: المفهوم والأسباب. الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الاقليمية والدولية، عمان، الاردن.

5) براهيم، عبد الحكيم مولاي. (2016) . الجرائم الالكترونية. مجلة الحقوق والعلوم الإنسانية، 2 (23)، 211،224.

6) الجريمة الالكترونية على النواحي الاقتصادية، صفحة بوابات كتابة أولاين. (http//nanaonline.com)-

7) حبابية، ميرفت محمد، ورابحي، لخضر. (2019) . أثر الجرائم الالكترونية على الاطفال وحمايتهم في ظل الاتفاقيات الدولية والتشريع الوطني الجزائري والفلسطيني. مجلة صوت القانون، 6(2)، 95 -112

8) حوحو، رمزيي، وبلورغي، منيرة. (2014). مواجهة الجريمة المعلوماتية في الجزائر. مجلة الحقوق والحريات، 2، جامعة محمد حيضر (بسكرة).

9) الدباجي، عبد الله سيف بن عيسى. (2013). مكافحة جرائم الاستغلال الجنسي للأطفال المرتكبة عبر الانترنت. أبوظبي: مركز بحوث الشرطة

10) رحموني، محمد. (2018). خصائص الجريمة الالكترونية ومجالات استخدامها. مجلة الحقيقة، 41، 432 451،

11) الرشيدي، محمود. (دت.). العنف في جرائم الأنترنت: أهم القضايا الحماية والتأمين. القاهرة: الدار المصرية اللبنانية.

12) سالم، محمد علي، هجيع، حسون عبيد. (2007). الجريمة المعلوماتية. مجلة جامعة بابل للعلوم الانسانية، 14 (2)، 85، 100

13) سليم، شاكر مصطفى. (1981). جريمة: قاموس الانثروبولوجيا. الكويت: دن.

14) الشكري، عادل يوسف عبد النبي. (2008). الجريمة المعلوماتية وأزمة الشرعية الجزائية. مجلة مركز دراسات الكوفة م1.ع7، ص ص، (111، 132).

15) عبد الخالق، جلال الدين، ورمضان، السيد (2001). الجريمة والانحراف من منظور الخدمة الاجتماعية. الإسكندرية المكتب الجامعي الحديث

16) عبد الفتاح، مراد. (2007) . شرح جرائم الكمبيوتر والانترنيث. الإسكندرية: دار الكتب والوثائق المصرية.

17) عليوة، سليم. (2021). الجريمة المعلوماتية. مجلة الأستاذ الباحث للدراسات القانونية والسياسية، 6(1). 1207 ، 1218.

18) المايل، عبد السلام محمد، الشربجي، وقابوسة، علي. (2019) . الجريمة الالكترونية في الفضاء الالكتروني. مجلة أفاق للبحوث والدراسات سداسية، 4، المركز الجامعي إليزي، 242 ،255.

19) المرزوق، خالد بن محمد سليمان. (2005). جريمة الاتجار بالنساء والأطفال وعقوبتها في الشريعة الاسلامية والقانون الدولي. رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية.

20) المشيخص، عبد العظيم نصر. (2005). الانحرافات الاجتماعية مشكلات وحلول. بيروت: دار الهدى للطباعة والنشر

21) المومني، نهلا عبد القادر. (2008). الجرائم المعلوماتية. عمان: دار الثقافة للنشر والتوزيع.

22) نيص، ليندا محمد، والزهيري، أشجان خالص. (2017). مبادئ علم الاجرام. عمان: دار الثقافة للنشر والتوزيع

23) Frank p ,Williams lll , &Marilyn D,McShane .(2013). Criminological Theory , https//cyberone.co

الجرائم الواقعة على البريد الإلكتروني

Offences against e-mail

ط.د. عبد النور قندسي /جامعة محمد الخامس، الرباط/المغرب
Abdenour Kandsi/ University of Mohammed V, Rabat/ Morocco

ملخص الدراسة:

البريد الإلكتروني يعتبر أحد أهم مفرزات الشبكة العنكبوتية، فإن أهميته تزداد يوما بعد يوم بازدياد عدد المتصلين بهاتة الشبكة، حيث أصبحت هذه الوسيلة على ما توفره من تسهيل الاتصال بين الأشخاص والمؤسسات، لا غنى عنها في الكثير من المجالات، فهي على صعيد الحياة الخاصة توفر للأفراد طريقة للاتصال المكتوب كبديل للرسالة والفاكس والتلغراف، والاتصال السمعي كبديل للهاتف

الكلمات المفتاحية: الشبكة العنكبوتية، البريد الإلكتروني، الحياة الخاصة، الاختراق، العنوان الإلكتروني

Abstract:

E-mail is one of the most important web detachments. Its importance increases day by day as the number of people connected to it increases. This means of facilitating communication between people and institutions is indispensable in many areas. In private, it provides individuals with a way of communication written as an alternative to message, fax and telegraph, and audio communication as an alternative to telephone.

Keywords: Web, e-mail, private life, hack, email address

مقدمة:

البريد الإلكتروني هو عبارة عن فضاء افتراضي داخل شبكة المعلومات، يحوزه شخص عن طريق اسمه قد يكون حقيقيا أو مستعارا، ولا يلج إليه إلا عن طريق رقم سري، ويستطيع الشخص من خلال هذا الفضاء الافتراضي الذي يحوزه أن يرسل أو يستقبل رسائل مكتوبة أو صوتية أو مصورة إلى شخص أو مجموعة من الأشخاص لديهم أيضا بريد إلكتروني على شبكة الانترنت، وذلك من خلال عبور هاته الرسائل إلى مقدم الخدمة على الشبكة لتصل إلى العنوان الإلكتروني المحدد على هاته الرسالة مباشرة إلى المرسل إليه إذا كان متصلا بالشبكة، أو تسجل عند الخادم في حالة عدم اتصال المرسل إليه بالشبكة Off line، وتبقى هناك حتى يتصل هذا الأخير بصندوق بريده الإلكتروني ويطلب جلب هذه الرسالة.

الأهداف:

الهدف مما ذكر أعلاه هو توفير الظروف المواتية المساهمة في إرساء مناخ ايجابي يتيح استعمال البريد الإلكتروني في جميع المعاملات خاصة التجارية دون تعرضه للاختراق.

مشكلة البحث:

وانطلاقا مما سبق نتساءل هل وضع المشرع المغربي نصوص قانونية كفيلة بحماية البريد الإلكتروني من كل اعتداء قد يصيبه؟

تتفرع عن هذه الإشكالية مجموعة من التساءلات:

ما المقصود بالبريد الإلكتروني؟ وما هي الجرائم التي يمكن أن ترتكب على البريد الإلكتروني؟

الفرضيات:

- ✓ يستعمل البريد الإلكتروني كبديل كامل عن المعاملات الورقية، سواء على مستوى الإدارات أو المقاولات التجارية، في إطار ما يطلق عليه الآن تسمية التجارة الإلكترونية.
- ✓ يعتبر البريد الإلكتروني وسيلة سريعة للاتصال، حيث لا تستغرق الرسالة أكثر من ثوان أو دقائق لتصل إلى المرسل إليه، بغض النظر عن مكان تواجده سواء كان في البلدة المرسل منها البريد الإلكتروني أو في دولة بعيدة.
- ✓ يمكن لمستعمل البريد الإلكتروني إرسال أكثر من رسالة لأكثر من شخص في وقت واحد.

المحور الأول: الاعتداء على البريد الإلكتروني

يعتبر التطور الهائل في الحياة السيبيرية قابله أيضا تطور تقنيات عدد كبير من الجرائم التقليدية ،حيث أصبحت ترتكب بشكل أسهل وبأقل جهد، ناهيك عن ظهور جرائم جديدة مرتبطة أساسا بهذا الفضاء الافتراضي، حيث أن الإحصائيات تشير إلى أرقام مخيفة (أحمد، 2007، صفحة 5)، وتكمن خطورة هذه الجرائم بداية في مرتكبها الذين يتسمون بالذكاء، حيث أنهم يستعملون وسائل التدمير الناعمة كالفيروسات والقنابل المنطقية، ولا يلجؤون إلى العنف كما هو الحال في الإجرام التقليدي، فهذا المجرم يكون في العادة خبيرا في أنظمة المعالجة المعلوماتية. (حجازي، 2002، صفحة 81) الأمر الذي يصعب من إمكانية تعقبه. كما أن الجرائم المعلوماتية التي تنصب بالأساس على البيانات ذات الطبيعة غير المادية تطرح العديد من المشاكل على المستوى العملي من حيث إثباتها وتعقب مرتكبها ،خاصة وأن الأدلة في هذا المجال سهلة المحو والإخفاء في زمن قصير ، كما أن المجرم يرتكب أفعاله عن بعد عبر الشبكة ولا يحتاج إلى التنقل إلى مسرح الجريمة وما يزيد في صعوبة مكافحة هذه الجرائم هو عدم التبليغ عن وقوعها، والسبب في ذلك يرجع إلى عدم اكتشافها أو عدم العلم بوقوعها أصلا، فقد قدرت إحدى الدراسات أن حوالي العديد من ضحايا جرائم الكمبيوتر لا يعلمون بأن أنظمتهم قد اخترقت والحري والتحقيق في هذا النوع من الجرائم، ذلك أن جرائم الكمبيوتر والانترنت تحتاج للكشف عنها وإثباتها ومعاقبة مرتكبها إلى أشخاص متخصصين في الإعلام الآلي والانترنت، وعلى دراية كافية بكل برامج القرصنة والفيروسات، كما يجب عليهم أن يحسنوا استعمال أجهزة

ولأن البريد الإلكتروني يعتبر أحد أهم مفرزات الشبكة العنكبوتية، فإن أهميته تزداد يوما بعد يوم بازدياد عدد المتصلين بهاته الشبكة، حيث أصبحت هذه الوسيلة على ما توفره من تسهيل الاتصال بين الأشخاص

والمؤسسات، لا غنى عنها في الكثير من المجالات، فهي على صعيد الحياة الخاصة توفر للأفراد طريقة للاتصال المكتوب كبديل للرسالة والفاكس والتلغراف، والاتصال السمعي كبديل للهاتف، وحتى الاتصال المصور بشكل مباشر وغير مباشر. أما على صعيد العمل فالبريد الإلكتروني يوفر للشركات الاتصال فيما بينها، وكذا الاتصال بالعملاء، ويوفر تبادل خطط وبرامج العمل، ويمكن من إبرام العقود والصفقات والاطلاع على التصاميم المختلفة، وهو الأمر ذاته على الصعيد العلمي، فالبريد الإلكتروني يسهل الاتصال بين الباحثين في عمليات الإشراف والمتابعة وتبادل المعلومات والآراء، وكل هذا وأكثر في ظرف ثوان أو دقائق معدودة، وهي المدة التي تستغرقها الرسالة الإلكترونية في الانتقال من أي مكان على الأرض إلى أي مكان آخر يكون متصلا بشبكة الانترنت.

أولا: مفهوم البريد الإلكتروني:

ظهر البريد الإلكتروني لأول مرة على يد العالم الأمريكي راي توملينسون صمم على شبكة الانترنت برنامج لكتابة الرسائل يسمى Send message، وذلك لتمكين العاملين على الشبكة من تبادل الرسائل فيما بينهم، ولم ينتظر طويلا ليخترع برنامج جديد أطلق عليه تسمية CYP net الذي يسمح بنقل الملفات من جهاز كمبيوتر إلى آخر، ثم دمج فيما بعد البرنامجين في برنامج واحد هو البريد الإلكتروني. ولأن الرسائل لم تكن تحمل اسم مرسلها فقد وضع توملنسون الرمز @ بين اسم المرسل والموقع الذي ترسل من أول عنوان بريد إلكتروني في التاريخ Tomlinson@bbn-tenexa

وقد عرف البريد الإلكتروني في بلده الأصلي الولايات المتحدة الأمريكية بتسمية E . Mail وهي اختصار للعبارة Electronic Mail، وترجم في اللغة الفرنسية إلى Courrier électronique، وقد عرف البريد الإلكتروني : SPAM (Solicited Pornography and Marketing. Guillaume Teissonnière , La lutte 33(contre le spamming : de la confiance en l'économie numérique à la méfiance envers ses acteurs, 2004) تعديلات وإضافات كثيرة، حيث ظهر البريد الإلكتروني الصوتي، وتقنية إرفاق الملفات السمعية والمرئية والمكتوبة، كما ظهرت تقنية حفظ الرسائل وترتيبها، وربط البريد الإلكتروني بقوائم العملاء والجهات المرسل إليها البريد بانتظام، كما طورت تقنية استقبال البريد الإلكتروني بواسطة المفكرات الإلكترونية المحمولة باليد وكذا عن طريق الهاتف النقال وهناك العديد من المواقع التي اشتهرت بتقديم خدمة البريد الإلكتروني. (Wahlert, 1998, p. 3)

وطريقة الاستفادة من خدمات البريد الإلكتروني سهلة وميسورة لكل من يحسن استخدام شبكة الانترنت، خاصة عند إنشاء هذا البريد على المواقع العامة التي تقدم هذه الخدمة مجانا، وهذا عن طريق إبرام عقد يسمى بعقد تقديم خدمة البريد الإلكتروني، وهي عبارة عن استمارة يملؤها المستفيد بمجموعة من البيانات الشخصية (قد تكون هذه البيانات سليمة أو غير ذلك) ،ويصادق على مجموعة من الشروط التي يفرضها مقدم الخدمة على الشبكة، ويدخل هذا العقد ضمن عقود الخدمات الإلكترونية، ويمكن أن ينشأ مستقلا أو ضمن عقود الخدمات الإلكترونية الأخرى.

– تعريف البريد الإلكتروني:

البريد الالكتروني : "وسيلة يتم بواسطتها نقل المراسلات الخاصة عبر شبكة خطوط تيلفونية عامة أو خاصة، وغالبا ما يتم كتابة الرسالة على جهاز كمبيوتر ثم يتم إرسالها إلكترونيا إلى كمبيوتر مورد الخدمة الذي يتولى تخزينها لديه

حيث يتم إرسالها عبر نظام خطوط التيلفون إلى كمبيوتر المرسل إليه"، كما عرف القانون الفرنسي الصادر في 22 جوان 2004، المتعلق بالثقة في الاقتصاد الرقمي الرسالة الإلكترونية على أنها: "كل رسالة سواء كانت نصية أو صوتية أو مرفق بها صور أو أصوات، ويتم إرسالها عبر شبكة اتصالات عامة، وتخزن عند أخد خوادم تلك الشبكة أو في المعدات الطرفية للمرسل إليه ليتمكن هذا الأخير من استعادتها"

أما التعاريف الفقهية فهي عديدة، نذكر منها بأن البريد الإلكتروني هو: "تلك المستندات التي يتم إرسالها واستلامها بواسطة نظام اتصالات بريدي إلكتروني، وتتضمن ملحوظات مختصرة ذات طابع شكلي حقيقي، ويمكنه استصحاب مرفقات به، مثل نظام معالجة أو أية مستندات أخرى يتم إرسالها رفقة الرسالة ذاتها"، كما عرف بأنه: "طريقة تسمح بتبادل الرسائل المكتوبة المتصلة بشبكة المعلومات،" وهو كذلك: "مكنة التبادل الإلكتروني غير المتزامن للرسائل بين أجهزة الحاسب الآلي"

وفي تقديرنا لهذه التعريفات، نشير إلى أنها تعريفات تقنية، تصب في مصب واحد مفاده أن البريد الإلكتروني هو عبارة عن فضاء افتراضي داخل شبكة المعلومات، يحوزه شخص عن طريق اسمه (قد يكون حقيقيا أو مستعارا)، ولا يلج إليه إلا عن طريق رقم سري، ويستطيع الشخص من خلال هذا الفضاء الافتراضي الذي يحوزه أن يرسل أو يستقبل رسائل مكتوبة أو صوتية أو مصورة إلى / من شخص أو مجموعة من الأشخاص لديهم أيضا بريد إلكتروني على شبكة الانترنت، وذلك من خلال عبور هاته الرسائل إلى مقدم الخدمة (الخادم، المقلم، Serveur على الشبكة لتصل إلى العنوان الإلكتروني المحدد على هاته الرسالة مباشرة إلى المرسل إليه إذا كان متصلا بالشبكة On line، أو تسجل عند الخادم في حالة عدم اتصال المرسل إليه بالشبكة Off line، وتبقى هناك حتى يتصل هذا الأخير بصندوق بريده الإلكتروني ويطلب جلب هذه الرسالة.

– مميزات وعيوب البريد الإلكتروني:

إن وسائل الاتصال بصورة عامة تعتبر من أكبر النعم على البشرية، بما تقدمه من خدمات جليلة في شتى المجالات، غير أننا نطرق باب معرفة مزايا وعيوب البريد الإلكتروني في سبيل المفاضلة بين هاته الوسيلة وغيرها من وسائل الاتصال من جهة، ومن جهة ثانية فإن عيوب وسائل الاتصال قد لا تكمن في الوسيلة ذاتها وإنما في سوء استخدامها على غرار ما هو موجود من فض للرسائل والاطلاع عليها والتنصت على المكالمات الخاصة في الوسائل التقليدية للاتصال، وعلى هذا سنتطرق في البداية إلى مزايا البريد الالكتروني، ثم نتطرق إلى عيوبه من خلال ما يلي:

أ –مميزات البريد الإلكتروني:

للبريد الإلكتروني العديد من المزايا التي حاولنا إجمالها فيما يلي:(داود، 2002، ص.24)

- ✓ يستخدم البريد الإلكتروني كبديل كامل عن المعاملات الورقية، سواء على مستوى الإدارات أو الشركات التجارية، في إطار ما يطلق عليه الآن تسمية التجارة الإلكترونية.

✓ يؤمن البريد الإلكتروني للأشخاص الطبيعية والمعنوية حاجياتهم دون عناء التنقل، وذلك من خلال طلب البضائع والاشتراك في الدوريات، بمجرد ذكر بيانات البطاقة الائتمانية، وهو ما يطلق عليه اليوم تسمية السوق الإلكترونية.

✓ يعتبر البريد الإلكتروني وسيلة سريعة للاتصال، حيث لا تستغرق الرسالة أكثر من ثوان[1] أو دقائق لتصل إلى المرسل إليه، بغض النظر عن مكان تواجده سواء كان في البلدة المرسل منها البريد الإلكتروني أو في دولة بعيدة.

✓ إن تكلفة البريد الإلكتروني لا تزيد عن تكلفة الاتصال بشبكة الانترنت، فهي لا تحتاج إلى رسوم أو طوابع ولا إلى مؤسسة توصيل، كما أن تكلفتها غير مرتبطة بطول أو قصر الرسالة، ولا بطول زمن الاتصال.

✓ إذا كان العنوان الإلكتروني المرسل إليه صحيحا فإن الرسالة لا تضل طريقها مثلما يحدث في البريد العادي.

✓ إن الشبكة العنكبوتية مصممة على ألا تتعرض للأعطال، وعلى ذلك فإن خدمة البريد الإلكتروني متوفرة طوال الوقت، فلا إجازة ولا عطل رسمية وغير رسمية، الأمر الذي يمكن مستعملي البريد الإلكتروني من إرسال بريدهم في أي وقت، ويقابل ذلك استقبال رسائلهم في أي وقت وكذا في أي مكان، طالما كانوا على اتصال بالشبكة وبريدهم متاح.

✓ كل الرسائل المرسلة أو المستقبلة تكون معنونة، وعليها تاريخ ووقت الإرسال والحفظ والاستقبال، وإن كان هذا التوقيت لا يتسم بالدقة المطلقة.

✓ يمكن لمستعمل البريد الإلكتروني إرسال أكثر من رسالة لأكثر من شخص في وقت واحد.

✓ إذا كان البريد الإلكتروني مأمنا بالشكل اللازم، فإن نسبة التطفل والاطلاع على ما فيه تتقلص بشكل كبير.

ب – عيوب البريد الإلكتروني:

ويمكننا أن نقسم هذه العيوب إلى عيوب متعلقة بالبريد الإلكتروني كوسيلة للاتصال، وعيوب متعلقة بإساءة استخدام هذه الوسيلة.

بالنسبة للعيوب المتعلقة بالبريد الإلكتروني كوسيلة اتصال، فإنه يمكننا حصرها فيما يلي:

✓ عدم إمكانية استعمال البريد الإلكتروني إلا من خلال جهاز معد لذلك كمبيوتر، هاتف نقال، مفكرة إلكترونية، ويجب أن يكون هذا الجهاز متصل بشبكة اتصال، وهو ما ينجر عنه أن تعطل هذه الشبكة أو عدم توفرها يعني عدم إمكانية إجراء الاتصالات المرغوبة.

✓ إن تخزين الرسائل الإلكترونية يتم في أكثر من مكان في صندوق البريد الإلكتروني مما قد يؤدي إلى مشاكل عملية التخزين.

✓ عدم وجود هيئة مسؤولة عن إدارة البريد الإلكتروني يتيح فرصة طبع الرسائل من خلال الانترنت بدون موافقة من جهة معينة، كما أن هناك إمكانية لحذف أو تعديل محتوى الرسائل الإلكترونية.

أما عن العيوب المتعلقة بإساءة استعمال البريد الإلكتروني فهي كثيرة نذكر منها ما يلي:

ثانيا: جرائم الاعتداء على البريد الإلكتروني (الاختراق والإغراق):

من خلال مداخلتنا ، تبين لنا أن البريد الإلكتروني (إبراهيم، 2008، الصفحات 53-54)تزداد أهميته في كل يوم وذلك بزيادة عدد المشتركين من جهة، وبزيادة أهمية وحساسية المعلومات المتبادلة من خلال جهة ثانية ،فمع زيادة أهمية البريد الإلكتروني تزداد أيضا خطورة الاعتداء عليه أو إساءة استعماله، فقد ظهرت في الوقت الحالي العديد من الجرائم المتعلقة بالبريد الإلكتروني، ويمكننا أن نصنفها ضمن فئتين أساسيتين؛ حيث تتضمن الفئة الأولى الجرائم المرتكبة بواسطة البريد الإلكتروني ،وهي كثيرة لا يمكننا حصرها، نذكر منها جريمة التهديد بالقتل، الابتزاز، النصب والاحتيال ،التحريض على القيام بأفعال جرمية، كالتحريض على الفسوق والدعارة والتحريض على القتل، التشهير والدعاية للإجرام، وكذا تبادل الرسائل بين المجرمين الدوليين،إرسال الصور والرسائل الماجنة، والترويج للمخدرات والإرهاب، وغير ذلك الكثير مما يمكننا أن نتصوره من أفعال يعتبر البريد الإلكتروني وسيلة لارتكابها، والملاحظ أن هذه الفئة من الجرائم يمكن إخضاعها لقواعد قانون الجنائي التقليدية، على الأقل من ناحية التجريم والعقاب.

أما الفئة الثانية من الجرائم المتعلقة بالبريد الإلكتروني، فهي الجرائم الواقعة على البريد الإلكتروني، ويمكننا حصرها في جريمتين أساسيتين هما: جريمة اختراق البريد الإلكتروني وتسمى أيضا بجريمة انتهاك سرية رسائل البريد الإلكتروني، وجريمة تضخيم البريد الإلكتروني وتسمى أيضا بجريمة الإغراق بالرسائل الإلكترونية، وسوف نتعرض لهاتين الجريمتين بالتفصيل من خلال ما يلي:

1 .جريمة اختراق البريد الإلكتروني :

الهجوم على المواقع واختراقها على شبكة الانترنت من الجرائم الشائعة في عصر المعلومات، وتشمل جرائم الاختراق تدمير المواقع، واختراق المواقع الرسمية والشخصية، واختراق البريد الإلكتروني أو الاستيلاء عليه، وكذا الاستيلاء على اشتراكات الغير وأرقامهم السرية،

ويمكننا أن نصنف الاختراق إلى ثلاثة أنواع وهي اختراق الأجهزة، اختراق المواقع، اختراق البريد الإلكتروني وهو ما يهمنا في هذه الدراسة، واختراق البريد الإلكتروني مفاده الدخول إلى البريد الإلكتروني والاطلاع على الرسائل الموجودة بداخله بدون إذن من صاحب البريد. من خلال هذا التعريف نجد أن جريمة البريد الإلكتروني ليست جريمة واحدة.

فهناك الاختراق وهناك أيضا انتهاك سرية رسائل البريد الإلكتروني، وفعل الاختراق قد يحتاج هو الأخر إلى ارتكاب جريمة أخرى كجريمة)الجهيني &الجهيني(2006, p. 46 , (الجهيني، 2006، ص.46) اصطياد كلمات المرور، أو استعمال إحدى برامج الاختراق التي تصنف على أنها برامج محظورة وغير شرعية.

والمهم في هذا المقام أن جميع جرائم الاختراق مع اختلافها إلا أنه يجمعها أمر واحد، وهو كونها جميعها تصب في مصب واحد هو انتهاك خصوصية الأشخاص، وهذا يعتبر سببا كافيا لتجريمها، بغض النظر عن الأضرار المادية والمعنوية التي تلحق بالمجني عليه.

فالخصوصية وإن لم تكن قضية تكنولوجية، فإنها تعتبر اليوم من أبرز القضايا الاجتماعية والأخلاقية في عصر تكنولوجيا الإعلام الآلي والانترنت، والاختراق يعد بمثابة انتهاك صريح للخصوصية بالخصوصية الإلكترونية E.privacy. وإن لم يكن هناك اتفاق حول مفهوم الخصوصية سواء، فإن الأمر الأكيد أن المراسلات بمختلف أنواعها تعتبر من بين الأمور الخصوصية للشخص، والتي لا يحق للغير الإطلاع عليها أو اعتراضها بأي وجه من الأوجه، ولا أدل على قولي هذا من أن مؤتمر رجال القانون الذي انعقد بستوكهولم في ماي 1967 قد عرف الحق في الخصوصية بأنه:

"حق المرء في أن يترك ليعيش حياته الخاصة بأقل درجات التدخل وحمايته من:

1. مراقبة مراسلاته،
2. الاستخدام السيئ لاتصالاته الشخصية الكتابية والشفوية،
3. استخدام المعلومات المأخوذة أو المعطاة بواسطته في حالات الثقة المهنية".
4. يؤكد الدستور على أنه: "لا يجوز انتهاك حرمة حياة المواطن الخاصة، وحرمة شرفه، ويحميهما القانون.
5. سرية المراسلات والاتصالات الخاصة بكل أشكالها مضمونة". [21]

حيث يمنع المساس بالحرية الشخصية وإطلاق حكم النص بتوظيف المؤسس الدستوري لعبارة "بكل أشكالها" يجعل من سرية مراسلات البريد الإلكتروني محمية دستوريا من أي اعتداء.

- ✓ بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة، أو سرية بغير إذن صاحبها أو رضاه،
- ✓ بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه،"

والملاحظ أنه إذا كانت الفقرة الأولى منسجمة مع نص المادة من الدستور وهذا في عبارة "كل من تعمد المساس بحرمة الحياة الخاصة للأشخاص بأي تقنية كانت"، غير أن المشرع لما بدأ في تعداد التقنيات المستعملة للمساس بالحياة الخاصة، أهمل التطرق للتقنيات المستعملة في الاعتداء على البريد الإلكتروني، حيث يفهم من هذا النص أن الأفعال المجرمة تنحصر في الاعتداء على المحادثات التليفونية، المحادثات الخاصة والسرية المباشرة، وأخذ صورة لشخص في مكان خاص. وحتى إن سلمنا بأن عبارة "الأحاديث الخاصة" تتسع لتشمل مراسلات البريد الإلكتروني، فإنها تنطبق على جزء من هذه المراسلات فقط (غرف الدردشة الخاصة) وليست كل المراسلات هذا من جهة، ومن جهة ثانية فإن القاضي الجنائي مقيد بمبدأ الشرعية ولا يجوز له القياس خاصة في مجال التجريم. (عيد03، 2008، صفحة 3)

التي جاء فيها أنه: "يعاقب... كل من أدخل بطريق الغش معطيات في نظام المعالجة الآلية أو أزال أو عدل بطريق الغش المعطيات التي يتضمنها".

[1]وإطلاق حكم النص بتوظيف المؤسس الدستوري لعبارة "بكل أشكالها" يجعل من سرية مراسلات البريد الإلكتروني محمية دستوريا من أي اعتداء.

نجد بأن هاتين المادتين تنصبان على تجريم الأفعال المنصبة على المساس بأنظمة المعالجة الآلية للمعطيات، وهو ما يطلق على تسميته جرائم الحاسب الآلي أو جرائم الكمبيوتر، حيث تقسم هذه الجرائم بحسب دور الكمبيوتر فيها إلى ثلاثة أنواع هي: الكمبيوتر هدف

للجريمة وهذا في حالة الدخول غير المصرح به إلى النظام، أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، أو الاستيلاء على البيانات المخزنة أو المنقولة عبر النظام. أما النوع الثاني فهو الحالة التي يكون فيها الكمبيوتر أداة لارتكاب الجريمة، ومثال ذلك استعمال الكمبيوتر في الاستيلاء على الأموال (تحويل الأرصدة) أو ارتكاب جرائم التزوير أو التأثير على برمجيات التحكم في الطائرات والسفن بشكل يؤدي إلى تدميرها وقتل ركابها. أما النوع الثالث فهو الحالة التي يكون فيها الكمبيوتر بيئة للجريمة، وهذا في حال تخزين البرامج التي تمت قرصنتها فيه، أو استخدامه لتخزين مواد غير قانونية أو إباحية كالترويج للمخدرات أو تحميل الصور الإباحية28. من خلال هذا التقسيم نلاحظ أن المادتين 394 مكرر و394 مكرر 1 وما بعدهما من قانون الجنائي لا تخرج عن النوعين الأول والثالث، أما النوع الثاني فإن العقاب على جرائمه يكون وفقا للنصوص التقليدية لقانون الجنائي.

والسؤال الذي يطرح في هذا المقام هو: ما هو المقصود بنظام المعالجة الآلية للبيانات؟ وعند بحثنا عن إجابة لهذا السؤال وجدنا بأن المعالجة الآلية للمعطيات أو البيانات هي كافة العمليات والمهام التي تخضع لها البيانات معطيات الكمبيوتر بما في ذلك إنشاؤها. (إبراهيم، 2008، صفحة 91) وإرسالها واستقبالها أو تخزينها أو تجهيزها على أي وجه آخر.

ويرى خبراء المنظمة الأوروبية للتعاون والتنمية الاقتصادية أن المقصود بالجريمة المعلوماتية هي كل سلوك غير مشروع أو مناف للأخلاق أو غير مسموح به يرتبط بالمعالجة الآلية للبيانات أو بنقلها. من خلال هذين التعريفين يمكننا القول بأن البريد الإلكتروني يندمج ضمن برامج أو أنظمة المعالجة الآلية للمعطيات، ومن ثمة فإن اختراق البريد الإلكتروني مجرم وفقا للمادة مكرر التي تنص على معاقبة "كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك"، فمجرد الدخول غير المشروع معاقب عليه، وكذا البقاء، بل وحتى المحاولة على ذلك معاقب عليها وإن كان من الصعب تصور إثبات المحاولة في مثل هذا النوع من الجرائم.

وإن كان هذا التحليل قد جرنا إلى أن اختراق البريد الإلكتروني مجرم في نصوص قانون العقوبات الجزائري، فإننا نعتقد أن مثل هذه التحليلات هي عبارة عن توسيع لمضمون النصوص الجنائية بما لا يوجد فيها صراحة، خاصة إذا علمنا أن القاضي الجزائي ملزم بمبدأ الشرعية الجنائية، ومن ثمة يجب ألا نحمل النصوص الجنائية ما لا تطيق من معنى، بل يجب على المشرع تدارك هذا النقص والعمومية في النصوص، والعمل على تطويرها وفقا لمتطلبات هذا العصر.

غير أنه وفي تحليل آخر وفقا لما قرره مجلس الشيوخ الفرنسي في إطار تحديده لمدلول النظام الآلي لمعالجة المعطيات في مشروع قانون غش المعلومات الفرنسي رقم لسنة 1988 الصادر في 05 جانفي 1988 الذي عرفه بأنه: "كل مركب يتكون من وحدة أو مجموعة وحدات معالجة تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة

الإدخال والإخراج وأجهزة الربط، والتي يربط بينها مجموعة من العلاقات التي عن طريقها يمكن تحقيق نتيجة معينة هي معالجة المعطيات أو التي تتضافر فيما بينها نحو تحقيق نتيجة معينة وهي معالجة المعطيات على أن يكون هذا المركب خاضع لنظام الحماية التقنية"، فقد حدد مجلس الشيوخ الشروط التي ينبغي أن تتحقق في وحدات النظام التي تحدد جانبا منها عبارة المجلس بأنه عبارة عن: مركب يتكون من وحدة أو مجموعة وحدات معالجة والتي تتكون كل منها من الذاكرة والبرامج والمعطيات وأجهزة الإدخال والإخراج وأجهزة الربط. والتي تكشف من جانب آخر عن أن النظام الآلي يتكون من عنصرين: الأول عنصر مادي يتكون من وحدة أو مجموعة من وحدات المعالجة أو الإدخال أو الإخراج أو الربط، والثاني عنصر من طبيعة غير مادية يتكون من البرامج والمعطيات تتضافر أو تتآلف فيما بينها من أجل تحقيق غاية محددة هي معالجة المعطيات. وبالتالي فإن الحديث هنا لا يخرج عن كون نظام المعالجة الآلية للبيانات لا يخرج عن جرائم الكمبيوتر وهي لا تتعدى وفقا لهذا التعريف إلى الجرائم الواقعة في حقل الانترنت، وهذا الاتجاه الثاني هو المرجح في تفسرنا لنصوص قانون العقوبات الجزائري ،وذلك بالنظر إلى الأهداف المسطرة في مشروع قانون الجنائي ، وما يؤكد توجهنا هذا هو استعمال المشرع لعبارة "المعالجة الآلية للبيانات" التي تمثل أول صور المعالجة الآلية، وهي أولى تطبيقات الكمبيوتر مع بداية ظهوره، لذا نفضل لو وظف المشرع عبارة نظام المعالجة الآلية للمعلومات للمعلومات .

– جريمة تضخيم البريد الإلكتروني:

يطلق على هذه الجريمة أيضا تسمية الإغراق بالبريد الإلكتروني SPAM وقد عرف الإغراق أو تضخيم البريد الإلكتروني بأنه: "تراسل نسخ مكررة بعدد كبير من نفس الرسالة عبر النظام التراسلي لبريد إلكتروني بما يترتب عليه عدم انتظام سير النظام التقني المعلوماتي"، كما عرف أيضا بأنه: "استقبال عدد كبير من الرسائل الإلكترونية المزعجة"34، ففي هذه الجريمة يقوم شخص أو مجموعة من الأشخاص بإرسال عدد كبير من الرسائل إلى البريد الإلكتروني لشخص ما بقصد الإضرار به، وهذا من خلال استخدام برامج متخصصة تعمل على استنساخ الرسالة الواحدة بشكل متكرر، وقد يصاحب هذه الرسالة فيروسات، أو صور وملفات كبيرة الحجم، حيث يؤدي هذا العمل إلى ملء المساحة المخصصة للبريد الإلكتروني للشخص المستهدف، وبالتالي تتعطل عنه الخدمة المقدمة من الشبكة ولا يستطيع استقبال أي رسالة، ورسائل الإغراق تستخدم للإضرار بمستخدم البريد الإلكتروني، والتي تصل إلى جهازه مرة واحدة فتؤدي إلى توقفه عن العمل على الفور، نظرا لما تسببه هذه الرسائل من ملء منافذ الاتصال أو ملء المساحة المتاحة لهذا الجهاز وكذا ملء قوائم الانتظار، الأمر الذي يترتب عنه انقطاع الخدمة وبالتالي تكبد خسائر مادية ومعنوية[1] تضخيم البريد الإلكتروني، حيث جاء في نص المادة أن: الفعل الذي بمقتضاه يتم إعاقة عمل نظام المعالجة الآلية للبيانات يعاقب عليه بالحبس والغرامة.

[1] وبالنظر إلى الضرر الهائل الذي يمكن أن تسببه رسائل الإغراق سواء بالنسبة للأشخاص الطبيعية أو المعنوية، فقد عملت العديد من التشريعات على تجريم هذا العمل غير المشروع، ففي الولايات المتحدة الأمريكية نذكر على سبيل المثال لا الحصر قانون مكافحة تضخيم البريد الإلكتروني لسنة 1989 المعدل في ماي 1990 لولاية واشنطن، وقانون ولاية أوهايو الصادر سنة 2002 الذي نص على تجريم رسائل البريد الإلكتروني مجهولة المصدر. أما في فرنسا فقد قام المشرع بتضمين قانون العقوبات الجديد نصا جرم فيه التعدي على قواعد البيانات

وبالرجوع إلى نص المادة الثانية وما بعدها في قانون الجنائي لا نجد أي نص يجرم إغراق البريد الإلكتروني، ولا وجود حتى لنص عام مماثل لما هو معمول به في التشريع الفرنسي يفيد أن أي عمل من شأنه تعطيل أنظمة المعالجة الآلية للمعطيات يترتب عليه العقاب، ذلك أن الفقرة الأخيرة من المادة مكرر تجرم تخريب نظام اشتغال المنظومة، والأمر الأكيد أن التخريب غير تعطيل نظام المعالجة، هذا إذا سلمنا بأن نظم المعالجة الآلية للمعطيات تتضمن معالجة البيانات والمعلومات على مستوى البريد الإلكتروني.

المحور الثاني: المرجعيات الدستورية والدولية

سنتطرق في هدا المحور للمرجعية الدستورية أولا، ثم المرجعية الدولية ثانيا.

أولا: المرجعية الدستورية.

لكنه بالرغم من كل هذه المبررات، فإن مشروع هذا القانون وإن كان قد تضمن في صيغته الحالية مقتضيات قانونية من شأنها أن تحصن فضاءات النشر على الشبكة العنكبوتية، خاصة فيما يتعلق بمكافحة جميع أشكال الجريمة الإلكترونية بعد مصادقة المملكة المغربية على اتفاقية بودابيست المتعلقة بالجريمة المعلوماتية بتاريخ: 29 يونيو 2018. فإنه لم يلق قبولا في صيغته الحالية من طرف الرأي العام الوطني، بل حتى من قبل بعض الأعضاء المعنيين بدارسه ومناقشة مضامينه في اجتماع مجلس الحكومة، حيث أن هذا الطرح يجد تفسيرا له ضمن فحوى مذكرة وزارة الدولة المكلفة بحقوق الإنسان والعلاقات مع البرلمان الموجهة إلى رئيس الحكومة بمراسلة عدد: 2020/115 بتاريخ: 27 مارس 2020، والتي أحيلت من طرف رئيس الحكومة على الأمين العام للحكومة بمراسلة إدارية عدد:685 المؤرخة في: 02 أبريل 2020. بالإضافة إلى ما ورد ضمن البلاغ الرسمي لمجلس الحكومة والذي أكد فيه أن "المجلس صادق على المشروع، على أن تتم مراجعته على ضوء ملاحظات السادة الوزراء من قبل لجنة تقنية وبعدها لجنة وزارية"، وهذا ما ينصرف إلى ما يفيد معناه أن هناك اعتراض على بعض مقتضياته من طرف بعض أعضاء الحكومة، وأن الصيغة النهائية للمشروع، بعد القيام بالتعديلات (المغربية، 2022) هي التي ستتم إحالتها على البرلمان، ويمكن مناقشتها وقبولها أو رفضها.

أما الفئة العريضة من المواطنين رواد مواقع التواصل الاجتماعي فقد عبروا عن رفض تام لمشروع هذا القانون، وطالبوا عبر تدوينات الفضاء الرقمي بسحبه نهائياً، وليس فقط بإدخال تعديلات عليه فحسب؛ كما كان النقاش سابقا بشأن موضوع المدونة الرقمية التي لم تجد طريقها ضمن مسار التشريع حينها. ومرد هاتهالمواقفالمعبر عنها بالرفض، هو اعتبار أن مشروع هذا القانون "يهدد بشكل صريح حرية الرأي والتعبير."لذلك ماهي المقتضيات المرجعية التي تضمن حرية الرأي والتعبير دستوريا، وما هو نطاق وحدود هاته الحرية في المعايير الدولية المعنية بحقوق الإنسان في هذا المجال؟

فبالرجوع إلى الوثيقة الدستورية لظهير 29 يوليوز 2011[1]، نجد أن المشرع المغربي قد سن مجموعة من المقتضيات التي تكرس حرية الرأي والتعبير من قبيل الفصل السادس من الدستور الذي نص على أن: "القانون هو أسمى تعبير عن إرادة الأمة. والجميع، أشخاصا ذاتيين أو اعتباريين، بما فيهم السلطات العمومية، متساوون أمامه، وملزمون بالامتثال له.وتعمل السلطات العمومية على توفير الظروف التي تمكن من تعميم الطابع الفعلي لحرية المواطنات والمواطنين، والمساواة بينهم، ومن مشاركتهم في الحياة السياسية والاقتصادية والثقافية والاجتماعية...". بالإضافة إلى ما تضمنه الفصل الخامس والعشرونفي مقتضياته التي تنص على أن "حرية الفكر والرأي والتعبير مكفولة بكل أشكالها. وحرية الإبداع والنشر والعرض في مجالات الأدب والفن والبحث العلمي والتقني مضمونة". وأخيرا الفصل الثامن والعشرون[2] الذي نص على أن "حرية الصحافة مضمونة، ولا يمكن تقييدها بأي شكل من أشكال الرقابة القبلية.وللجميع الحق في التعبير، ونشر الأخبار والأفكار والآراء، بكل حرية، ومن غير قيد، عدا ما ينص عليه القانون صراحة.وتشجع السلطات العمومية على تنظيم قطاع الصحافة، بكيفية مستقلة، وعلى أسس ديمقراطية، وعلى وضع القواعد القانونية والأخلاقية المتعلقة به."...

ثانيا: المرجعية الدولية

وبخصوص أهم المرجعيات الدولية لحقوق الإنسان في مجال حرية الراي وحرية التعبير، فإنها ترتكز بالأساس على ما ورد في المادة 19 من الإعلان العالمي لحقوق الإنسان، والمادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسة، التي وضعت الإطار العام لممارسة حرية الراي وحرية التعبير بمختلف الوسائل بما فيها استخدام شبكات التواصل الاجتماعي والبث المفتوح، وهو ما أكدته الجمعية العامة للأمم المتحدة في قرارها 167/68 ومجلس حقوق الإنسان في قراريه 13/26 و 13/32 عندما اعتبر أن حرية التعبير والحقوق الأخرى تنطبق على شبكة الأنترنيت، والتعليق العام رقم 34 للجنة المعنية بحقوق الانسان التي اعتبرت أن "حرية الرأي وحرية التعبير شرطان لا غنى عنهما لتحقيق النمو الكامل للفرد، وهما عنصران يشكلان حجر الزاوية لكل مجتمع تسوده الحرية والديمقراطية، وشرطا كذلك لإرساء مبادئ الشفافية والمساءلة التي تمثل بدورها عاملا اساسيا لتعزيز حقوق الإنسان وحمايتها.

إن كل هذه المعايير والتقارير الموازية والاتفاقيات المصادق عليها[3]، تؤكد بشكل صريح على أن الدول يجب أن تلتزم بحماية جميع أشكال التعبير ووسائل نشرها بما فيها الأشكال السمعية البصرية ووسائل التعبير الإلكترونية والشبكية. (الرابط:، 2017) وفي مقابل ذلك، فإن القيود المسموح بها للدول للحد من هذه الحرية هي استثناء من

[1]ظهير شريف رقم 1.96.157 صادر في 23 من جمادى الأولى 1417(7 أكتوبر 1996) بتنفيذ نص الدستور

[2]أضيف هذا الباب بمقتضى المادة الفريدة من القانون رقم 07.03 بتتميم مجموعة القانون الجنائي فيما يتعلق بالجرائم المتعلقة بنظم المعالجة الآلية للمعطيات، الصادر بتنفيذه ظهير شريف رقم 1.03.197 بتاريخ 16 من رمضان 1424 (11 نوفمبر 2003)؛ الجريدة الرسمية عدد 5171 بتاريخ 27 شوال 1424 (22 ديسمبر 2003)، ص 4284.

[3]تم اعتماد الاتفاقية وتقريرها التفسيري من لدن لجنة وزراء مجلس أوروبا في دورتها التاسعة بعد المائة (8 نوفمبر/تشرين الثاني 2001 (وفتح باب التوقيع على الاتفاقية في بودابست، في 23 نوفمبر/تشرين الثاني 2001، بمناسبة المؤتمر الدولي حول الجريمة الإلكترونية، وقد صادق عليها المغرب وقام بإيداع وثائقها لدى أمانة مجلس أوروبا بتاريخ 29 يونيو 2018، وأصبحت مقتضيات هذه الاتفاقية منذ تاريخ فاتح أكتوبر 2018 جزءً من القانون الوطني.

القاعدة العامة التي تكرس الحرية، وتندرج هذه القيود في أمرين: أولهما أن تكون هذه القيود بمقتضى القانون، وثانيهما أن تختص بمجالين اثنين: حيث تكون في المجال الأول ضرورية لاحترام حقوق الأخرين وسمعتهم، وأن تكون في المجال الثاني ضرورية لحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة. لكن هذه الاستثناءات الواردة على حرية التعبير يجب أن تخضع لمجموعة من الضوابط المتمثلة فيما يلي:

- ✓ أن تكون الاستثناءات متلائمة مع اختبارات صارمة، تتعلق بالضرورة والتناسب؛
- ✓ ألا تستعمل لتبرير كبح أي دعوة إلى إقامة نظام ديمقراطي وتحقيق مبادئ ديمقراطية وحقوق الإنسان؛
- ✓ ألا يمنح القانون للأشخاص المسؤولين عن التنفيذ سلطة تقديرية مطلقة في تقييد حرية التعبير؛
- ✓ ألا تكون وسيلة للقمع أو لحجب معلومات عن الجمهور أو لمقاضاة الصحفيين أو الباحثين أو الناشطين أو المدافعين عن حقوق الإنسان أو أشخاص آخرين لأسباب تتعلق بنشر تلك المعلومات؛
- ✓ ألا يشمل اختصاص هذه القوانين فئات من المعلومات، كالفئات المتعلقة بالقطاع التجاري أو القطاع المصرفي أو التقدم العلمي؛
- ✓ ألا تكون القيود المفروضة مفرطة وأن تتماشى مع مبدأ التناسب، لتحقيق وظيفتها الحمائية، ومتناسبة مع المصلحة التي ستحميها، وأن يراعي مبدأ التناسب شكل التعبير موضوع النظر فضلا عن وسائل نشره؛
- ✓ ألا يشمل الحظر ممارسة المعارضة السياسية ونقد الشخصيات العامة وما يتصل بذلك؛
- ✓ ألا تنبني قواعد المنع والحظر والترخيص على التمييز بين المعنيين بمجال الصحافة والنشر، سواء كانوا صحافيين أو محللين أو أصحاب مدونات إلكترونية وغيرهم ممن يشاركون في أشكال النشر الذاتي المطبوع أو على شبكة الأنترنيت؛
- ✓ تجنب المعاقبة على بيانات غير صحيحة نشرت خطأ بدون نية سيئة؛
- ✓ ألا يتم تطبيق القانون الجنائي إلا في أشد الحالات خطورة، وألا تكون عقوبة السجن على الإطلاق هي العقوبة المناسبة؛
- ✓ ألا ينبغي إرغام مقدمي الخدمات على كشف بيانات المستخدمين إلا بأمر من السلطات القضائية، يثبت الضرورة والتناسب بغية تحقيق هدف مشروع

أما المجلس الوطني لحقوق الإنسان باعتباره مؤسسة وطنية دستورية، فقد أورد في تقريره السنوي الأخير بأنه" رصد خلال سنة 2019 عددا من المتابعات القضائية بسبب نشر مضامين في الفضاء الرقمي، خاصة عبر شبكات التواصل الاجتماعي، حيث يسجل المجلس بانشغال إدانة بعض هؤلاء المتابعين بعقوبات سالبة للحرية، وبالخصوص في أشكال التعبير التي تحظى بالحماية في المنظومة الدولية لحقوق الإنسان. وفي هذا السياق، فقد أوصى في تقريره، بخصوص حرية الرأي والتعبير، ومن ضمنها حرية الصحافة.

خاتمة:

نخلص في نهاية هذه المداخلة، أن التطور التكنولوجي الكبير في مجال المعلومات الذي أسهم بشكل كبير في رخاء البشرية في جوانب عديدة من الحياة، هو نفسه الذي وفر ملاذا أكثر أمانا لنوع جديد من المجرمين، وهيأ مجالا خصبا لنمو جرائم جديدة تتسم بالنعومة في ظاهرها وبالخطورة الشديدة في نتائجها المدمرة.

وإن كنا قد ركزنا في هذه الدراسة على جرائم البريد الإلكتروني، فهذا لا يعني أن الجريمة الإلكترونية منحصرة فيها، فهناك كم هائل من الأفعال الجرمية التي وجدت في فضاء الانترنت مرتعا لها، وهي في تطور وتزايد مستمر، إلا أن الاعتداء على البريد الإلكتروني يمثل اعتداء على جانب مهم في حياتنا اليومية ألا وهو الحق في الخصوصية، وتحديدا الحق في سرية المراسلات والاتصالات.

- ✓ تجميع كافة المقتضيات التشريعية ذات الصلة بالصحافة في مدونة النشر
- ✓ عدم مساءلة المبلغين والمصادر الصحفية إلا في الحالات المنصوص عليها قانونا واعتماد سياسات ترتكز على الشفافية لتمكين العموم من الولوج إلىالمعلومة، خاصة تلك التي تهم المصلحة العامة ولا تمس بالأمن القومي والحياة الخاصة للأفراد؛
- ✓ دعوة السلطات القضائية إلى التشبث بمبدأ يالضرورة والتناسب بما لا يمس الحق في حرية التعبير وحرية الصحافة وجعلهما في منأى عن كل عقوبة سالبة للحرية؛
- ✓ تعديل جميع أحكام القانون الجنائي المتصلة بموضوع حرية التعبير، بما يتوافق مع المادة 19 من العهد الدولي الخاص بالحقوق المدنية والسياسية، والحرص على أن يكون أي قيد مفروض على هذه الحرية محددا بنص قانوني صريح ومتاح، وأن تكون هذه القيود ضرورية لاحترام حقوق الآخرين أو سمعتهم، وحماية الأمن القومي أو النظام العام أو الصحة العامة أو الآداب العامة؛
- ✓ فتح نقاش عمومي حول "حرية التعبير والرأي والصحافة" ينخرط فيه جميع الفاعلين المعنيين ويأخذ بعين الاعتبار التحولات المرتبطة بهذا الموضوع، خاصة في الفضاء الرقمي، ولا سيما منصات التواصل الاجتماعي، بما يكفل هذه الحرية دون المساس بالحياة الخاصة للأفراد.

قائمة المراجع:

1) التقرير السنوي للوكالة الوطنية لتقنين المواصلات لسنة 2017، ص: 18، منشور على الرابط.https://www.anrt.ma/sites/default/files/rapportannuel/rapport_annuel_2017_va.pdf

2) الجهيني، منير محمد، والجهيني، وممدوح محمد. (2006). جرائم الانترنت والحاسب الآلي ووسائل مكافحتها.الإسكندرية: دار الفكر الجامعي

3) حسن، طاهر داود. (2000). جرائم نظم المعلومات، الرياض-السعودية-، أكاديمية نايف العربية للعلوم الأمنية.

4) خالد، ممدوح إبراهيم. (2008). أمن مراسلات البريد الإلكتروني، الإسكندرية: الدار الجامعية.

5) عارف، خليل أبو عيد. (2008). جرائم الأنترنت دراسة مقارنة". مجلة جامعة الشارقة للعلوم الشرعية والقانونية، 05(3).

6) عبد الفتاح بيومي حجازي. (2002). النظام القانوني لحماية التجارة الإلكترونية. الإسكندرية: دار الفكر الجامعي.

7) الموقع الرسمي لرئيس الحكومة /https://www.cg.gov.ma: تاريخ الاطلاع:10 أبريل2022، على الساعة العاشرة والنصف صباحا

8) هلالي، عبد اللاه أحمد. (2007). جرائم المعلوماتية عابرة الحدود. القاهرة: دار النهضة العربية.

Glenn, Wahlert,(1998) Crime in cyberspace : trends in computer crime in Australia, presented at the conference : internet crime, Melbourne, by the Australian institute of criminology.

Juriscom(2 avril, 2004) SPAM . Solicited Pornography and Marketing. Guillaume Teissonnière, La lutte 33(contre le spamming: de la confiance en l'économie numérique à la méfiance envers ses acteurs, (sign in 16/03/2022) available on, http://www.juriscom.net.





المؤتمر الدّولي العلمي الافتراضي بعنوان:

الجرائم الإلكترونية في الفقه الإسلامي والقانون الوضعي

Cybercrime in Islamic jurisprudence and positive law

رئيس المركز الديمقراطي العربي: أ. عمار شرعان

مدير النشر: د. أحمد بوهكو

رقم تسجيل الكتاب

VR .3383-6628 B

جوان 2022


الدراسات الإستراتيجية والسياسية والاقتصادية
D.A.C
المركز الديمقراطي العربي